指数和的估计
及其在数论中的应用

华 罗 庚 著



科 学 出 版 社

內 容 簡 介

本书主要討論了指数和的各种估計方法及其应用，特别討論了这些方法对 Waring 問題及 Гольдбах 問題的应用．除此而外，也談到了解析数論的其他一些問題与方法．本书不仅綜合了这几方面的結果与文献，更重要的是对其中絕大部分重要的結果都給出了較完备的提綱性的証明．本书对于想了解这方面数学成果及从事这方面研究工作的数学工作者，将会有所帮助．

指数和的估计
及其在数論中的应用

华 罗 庚 著

*

科学出版社出版（北京朝陽門大街 117 号）

北京市书刊出版业营业許可証出字第 061 号

中国科学院印刷厂印刷　新华书店总經售

*

1963 年 8 月第 一 版　　书号：2767

1963 年 8 月第一次印刷　　字数：153,000

（京）精：1—2,700　　开本：787×1092 1/18

平：1—2,900　　印张：7 7/9　插頁：3

定价：精裝本 1.90 元
平裝本 1.20 元

序

“指数和的估計及其在数論中的应用”一书是应“德国数学百科全书”編委会之請而写，作为这套书的一个分册于 1959 年在德国以德文出版.

本书的目的在于系統地总結指数和方法. 近代解析数論、几何数論与堆垒数論所以有如此重大的发展，都是由于指数和方法的引入与改进. 尤其是著名的素数分布問題，Waring 問題，Гольдбах 問題，Tarry 問題以及圓內、球內整点問題等，更加如此.

作为百科全书的一部分，本书力求較全面地介紹这一分支的工作. 不仅如此，本书的写作方法，还不只是結果与文献的罗列，而是尽力注意到这一分支的系統性、关联性与完整性. 我試图把主要結果貫穿起来，并且尽可能地扼要地涉及到这些結果的証明. 希望有一定数学修养的讀者，可以直接看懂本书的主要部分，而不必另翻原作. 以上是作者平素对总結性与綜合性文章的撰写要求，虽然由于篇幅有限以及作者知識水平的局限，未能完全如愿，但作者还是尽力为之的.

本书由 1952 年开始撰写，至 1956 年完稿，自始至終是在中国科学院数学研究所党組織的支持与鼓励下进行工作的. 飲水思源，衷心感謝. 在写作过程中，很多同志帮我查閱了可能得到的文献，并且編制了附有摘要的文献卡片. 而本书就是在掌握这些材料之后，經整理、消化、取舍与綜合，而后写成的. 作者謹向这些同志致以謝意.

五年来，这一分支又有了进一步的发展. 王元、吳方两同志在翻譯本书的同时，又写了五个附录，把最近发展的結果补充了进去.

最后，作者衷心地希望讀者多提意見与批評.

華罗庚

1963 年 1 月

目　　录

导　　引

堆垒数論的历史是从两个著名的問題,即 Гольдбах 問題与 Waring 問題开始的.

Гольдбах 問題是在 1742[1] 年, Гольдбах 写信給 Euler 时提出的. 在信中, Гольдбах 提出了关于将整数表为素数和的两个猜想. 这两个猜想可用略为修改了的語言叙述为:(A)每一个 $\geqslant 6$ 的偶数都是两个奇素数之和;(B)每一个 $\geqslant 9$ 的奇数都可以表成三个奇素数之和. 显然,由命題(A)可以推出命題(B).

从 Гольдбах 写信起到今天,已經积累了不少宝貴的数值資料[2]. 这些資料指出了这两个猜想是正确的,但迄今还不能証明它們的眞伪.

大約在四十年前[3],即使是証明如下的命題: 存在一个整数 c, 使每一个 $\geqslant 2$ 的整数都可表为不超过 c 个素数之和,也被認为是現代数学家力所不能及的事.

在 1770 年, Waring 提出了下面的猜想[4]:每一个自然数都是四个平方之和,九个立方之和,十九个四方之和,等等. 他的言論表明了他相信:对于每一个給定的整数 $k \geqslant 2$, 恆存在一仅依賴于 k 的整数 $s = s(k)$, 使每一正整数都可表为不超过 s 个非負整数的 k 次方之和.

Hilbert[5] 在 1909 年 (Waring 提出猜想后的 139 年) 首先証明了 $s(k)$ 的存在性. 以后, Шнирельман[6] 又在 1930 年 (Гольдбах 提出猜想后的 188 年) 証明了 c 的存在性. Hilbert 的方法虽然是很奇妙的,但它在堆垒素数論的近代发展中,并未显示出其功效. 但另一方面, Шнирельман 方法是广有用途的. 我們可以用这一方法同时处理这两个問題. 更須指出,在 Шнирельман 的論文中,他引入了关于自然数集合的非常重要的概念——“正密率”.

Hardy 与 Littlewood 在这一世紀的二十年代,作出了极为重要的貢献. 用他們強有力的方法,不仅能够得到关于存在性的結果,而且可以得到明确的上界. 在总标題为“‘partitio numerorum’ 的若干問題”[7]的一系列論文中,他們系統地开創与发展了堆垒数論中的一个嶄新的解析方法. 这个方法就是人所共知的 Hardy 与 Littlewood 的圓法[8]. 命 $G(k)$ 表示最小的整数 s,使每一充分大的整数都能表成 s 个非負整数的 k 次方之和. 圓法可以得出 $G(k)$ 的一个明确的上界. 同时他們在广义 Riemann 猜想之下,証明了每一充分大的奇数都可以表为三个素数之和. Landau[9] 把这些結果都很好地整理在他的专著之中了.

为了取消在証明 Гольдбах 問題时所用到的未經証明的猜想,并改进 Waring 問题中的上界 $G(k)$,我們需要估計某种类型的指数和(Виноградов 称它們为三角和). 因此，获得指数和的精确估計就成了近代堆垒数論的解析方法发展中的最主要环节了. 在近三十年来，Виноградов 創造了一系列估計指数和的天才方法. 因此,他对 Hardy-Littlewood 方法作了巨大的改进:

对于 Гольдбах 問題，Виноградов 成功地对某种以素数为变数的指数和給出了非无聊的估計,他証明[10] 了命題(B)对于充分大的奇数是正确的. Бороздкий[11] 經过計算証明了,每一奇数 $n \geqslant e^{e^{16.038}}$ 都能表成三个奇素数之和.

后来，Линник[12] 沿用 Hardy-Littlewood 原来的方法，并借助于 Dirichlet L-函数的零点的知識,亦証明了同样的結果.

另外一个研究 Гольдбах 問題的方法就是"篩法". 这一方法是 Erathostenes[13] 首創的. Brun[14] 与 Selberg[15] 分别对这一方法作出了重要的改进. 由这一方法所得到的最好的、已經发表的結果是[16]：每一充分大的偶数都是两个素因子个数各不超过 3 的整数之和. 但是无論如何，Selberg[17] 曾經宣布过,用他的方法可能証明每一充分大的偶数都可表为一个不超过 2 个素数的乘积及一个不多于 3 个素数的乘积之和. 此外,应用 Линник[18] 的大篩法，Renyi[19] 証明了：每一充分大的偶数都是一个素数及一个素因子个数不超过某一給定常数的整数之和.

我們称在 Waring 問題的研究中所遇到的指数和为 Weyl 和. Weyl[20] 在关于一致分布的开創性工作中,最先使用了这种和. 因此,他也是首先給出这种和以非无聊估值的人. 他的估計成了 Hardy-Littlewood 关于 Waring 問題的研究方法中的一个最主要环节. Виноградов 与 van der Corput 作出了关于估計这种和的重要貢献.

Виноградов[21] 在 1935 年发表了一系列关于 Weyl 和的論文，他不断地改进着自己的結果. 他的方法的最后形式被收集在他的选集[22]之中. 在华罗庚[23]的专著中也有着 Виноградов 方法的略为改进了的形式. Виноградов 方法的价値不仅在于它能成功地用于 Waring 問題,而且它还有效地应用于素数分布論，Riemann ζ-函数論及 Dirichlet L-函数論，一致分布及 Diophantine 逼近論，高維椭球中的格子点估計及 Prouhet 問題等等. 例如,用 Виноградов 的結果可以証明,不超过 x 的素数个数等于

$$\operatorname{li} x + O(xe^{-c(\log x)^{3/5}})^{24)}.$$

我們称下面的問題为 Prouhet 問題[25] (有时也称为 Tarry 問題或 Tarry-Escott 問题),即寻求最小的整数 s，使不定方程組

$$x_1^h + \cdots + x_s^h = y_1^h + \cdots + y_s^h, \quad 1 \leqslant h \leqslant k$$

有非无聊解,也就是說，$x_1, \cdots, x_s$ 不是 $y_1, \cdots, y_s$ 的重新排列. 华罗庚[26]指出:估

計 Prouhet 問題的解数是 Виноградов 方法的主要环节；另一方面，这一方法也能用于 Prouhet 問題.

改进 $G(k)$ 上界的另一重要环节是寻求方程

$$x_1^k + \cdots + x_l^k = y_1^k + \cdots + y_l^k$$

的解数的上界,此处 x 与 y 都是适合某些条件的整数.

Виноградов[27] 証明了 $G(k) \leqslant 3k \log k + 11k$，而 Davenport[28] 則对較小的 k 作出了重要的貢献. $k = 3$ 时，較好的估計 $G(3) \leqslant 7$ 則是属于 Линник[29] 的. 运用 Виноградов 強有力的方法，Dickson[30]，Pillai[31] 与 Niven[32] 証明了：当 $k \neq 4$ 与 5，$k > 3$ 及 $\left(\frac{3}{2}\right)^k - \left[\left(\frac{3}{2}\right)^k\right] \leqslant 1 - \left(\frac{1}{2}\right)^k \left\{\left(\frac{3}{2}\right)^k + 3\right\}$ 时,每一整数都能表成 $g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$ 个非負整数的 k 次方之和. Siegel[33] 則将 Hardy–Littlewood 的圓法推广到代数数域上去.

Van der Corput[34] 給出了估計 Weyl 和的另一方法. 这一方法对圓內整点問題、除数問題与几何数論的其他問題,以及 Riemann ζ-函数論中的 Lindelöf 猜想,都有着重要的应用. 以后,他本人，Titchmarsh 与 Виноградов 又推广与改进了这个方法.

关于 L-函数及模函数論，請讀者参看百科全书中另一些专著“特殊的 Dirichlet 級数及其应用”与“解析数論中的模函数論”. 同样,本书亦不包括超越数論及 Diophantine 逼近論. 关于这些主題,可以参看熟知的 Siegel，Гельфонд 与 Koksma 的书(見后面的参考书籍).

Erdős 教授，Линник 教授与 Turán 教授都对本书提供了宝貴的意見，作者仅向他們致以衷心地感謝. 在准备这本书的手稿时,又得到了越民义先生与王元先生的帮助,作者也借此机会向他們致以謝意.

第一章　初等方法

1. 密　率

命$\mathfrak{A}$表一由一些互不相同的非負整数a所成的集合. 命$A(n)$表$\mathfrak{A}$中不大于n之正整数的个数,即$A(n)=\sum_{1\leqslant a\leqslant n}1$,在此需要注意0并不計算在內. 若$\alpha>0$为使$A(n)\geqslant\alpha n$对于一切$n\geqslant1$都成立的最大正数,則称$\mathfrak{A}$具有正密率$\alpha$. 显然$\alpha\leqslant\leqslant1$. 若$\alpha=1$,則$\mathfrak{A}$包有全体自然数. 引入記号$\mathfrak{B}$, b, $B(n)$, β及$\mathfrak{C}$, c, $C(n)$, γ,其間之关系一如$\mathfrak{A}$, a, $A(n)$, α.

所有形如$a+b$ ($a\in\mathfrak{A}$, $b\in\mathfrak{B}$)的整数所成之集合$\mathfrak{C}$,称为$\mathfrak{A}$与$\mathfrak{B}$的"和集",記为$\mathfrak{C}=\mathfrak{A}+\mathfrak{B}$. 关于$\mathfrak{A}$与$\mathfrak{B}$的和集$\mathfrak{C}$, Шнирельман[6]很簡单地証明了下面两个重要定理:

(A) 若$0\in\mathfrak{A}$,則$\gamma\geqslant\alpha+\beta-\alpha\beta$;

(B) 若$0\in\mathfrak{A}$及$\alpha+\beta\geqslant1$,則$\gamma=1$,即集合$\mathfrak{C}$包有全体自然数.

命$2\mathfrak{A}=\mathfrak{C}=\mathfrak{A}+\mathfrak{A}$,并用归納法定义$s\mathfrak{A}=\mathfrak{A}+(s-1)\mathfrak{A}$,則由(A)可知,$s\mathfrak{A}$的密率$\geqslant1-(1-\alpha)^s$. 命$s_0=\left[\frac{\log 2}{\log\frac{1}{1-\alpha}}\right]+1$,則$s_0\mathfrak{A}$的密率$\geqslant\frac{1}{2}$. 又由(B)可知,集合$2s_0\mathfrak{A}$包有全体自然数,故得:

(C) 若$\mathfrak{A}$包有0,則每一正整数都可表成$\mathfrak{A}$中$2s_0$个元素之和.

Шнирельман給出了集合具有正密率的判别法:

(D) 命$\mathfrak{A}^*$表一非負整数之集合,其中的元素允許重复,命$\mathfrak{A}$为$\mathfrak{A}^*$中不同元素所成之最大集合. 命$r(a)$表示a在$\mathfrak{A}^*$中出現之次数. 若有$\alpha'>0$,使对諸$n\geqslant1$都有

$$\frac{1}{n}\left(\sum_{1\leqslant a\leqslant n}r(a)\right)^2\geqslant\alpha'\left(\sum_{1\leqslant a\leqslant n}r^2(a)\right),$$

則$\mathfrak{A}$有正密率$\alpha\geqslant\alpha'$.

事实上,由 Буняковский-Schwarz 不等式可知

$$\left(\sum_{1\leqslant a\leqslant n}r(a)\right)^2\leqslant\sum_{1\leqslant a\leqslant n}r^2(a)\sum_{1\leqslant a\leqslant n}1=A(n)\sum_{1\leqslant a\leqslant n}r^2(a).$$

以上就是 Шнирельман 关于正整数集合的貢献的主要部分.

命 $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_s$ 为密率都是 α 的 s 个集合. Хинчин[35] 証明了:集合 $\mathfrak{A}_1+\mathfrak{A}_2+ +\cdots+\mathfrak{A}_s$ 的密率 $\geqslant \min(1, s\alpha)$.

Mann[35] 在 1942 年証明了重要的猜想: $\gamma \geqslant \min(1, \alpha+\beta)$. 以后, Artin 与 Scherk[37] 又簡化了 Mann 的証明. 請讀者参考 Ostmann[38] 的书,在那里詳細地闡述了密率的理論及其应用.

2. Hilbert-Waring 定理

在講 Линник[39] 关于 Hilbert-Waring 定理的初等証明之前(在此稍有簡化与改进[40]),先証明下面两个引理.

引 1. 命 $X, Y \geqslant 0$. 又命 $q(n)$ 为不定方程

$$x_1y_1 + x_2y_2 = n, \quad |x_m| \leqslant X, |y_m| \leqslant Y, \quad m = 1, 2, \tag{1}$$

的整数解数,则

$$q(n) \ll \begin{cases} (XY)^{\frac{3}{2}}, & \text{若 } n = 0; \\ (XY)\sum\limits_{d|n}\dfrac{1}{d}, & \text{若 } n \neq 0. \end{cases} \tag{2}$$

当 $n=0$ 时,引理显然成立. 当 $n \neq 0$ 时,只要証明在条件 $(x_1, x_2)=1$ 及 $|x_2| \leqslant |x_1| \leqslant X$ 下,(1)的解数 $q'(n) \ll XY$ 即可. 不失一般性,可以假定 $X \leqslant Y$. 命 y_1', y_2' 是(1)的一組解答,則其他解 y_1, y_2 可以表成 $y_1 = y_1' + tx_2$, $y_2 = y_2' - tx_1$. 因此 $|t| = \dfrac{|y_2'-y_2|}{|x_1|} \leqslant \dfrac{2Y}{|x_1|}$. 所以

$$q'(n) \leqslant \sum_{1\leqslant|x_1|\leqslant X}\ \sum_{|x_2|\leqslant|x_1|}\frac{5Y}{|x_1|} \ll XY.$$

由引理立刻推出

$$\sum_{|a|\leqslant 2XY} q^2(a) \ll (XY)^3. \tag{3}$$

引 2. 命 $k \geqslant 2$ 及

$$f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x, \quad a_k \ll 1, \quad a_{k-1} \ll P, \quad \cdots, \quad a_1 \ll P^{k-1}$$

为一整系数多項式,则

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll P^{8^{k-1}-k}, \tag{4}$$

此处与記号 $\ll$ 有关的常数仅依賴于 k.

仅仅是为了方便,我們才在这里使用了积分. 我們可以毫无困难地把全部証明

都用初等数論的語言写出来.

当 $k=2$ 时,(4)之左端乃方程

$$f(x_1)+f(x_2)-f(y_1)-f(y_2)=f(x_3)+f(x_4)-f(y_3)-f(y_4),$$
$$x_m \ll P;\quad y_m \ll P;\quad m=1,2,3,4$$

的整数解数. 显然它不超过方程

$$z_1w_1+z_2w_2=z_3w_3+z_4w_4,\quad z_m \ll P;\quad w_m \ll P,\quad m=1,2,3,4$$

的整数解数. 因此,由(3)可知,引理当 $k=2$ 时是正确的. 現在用归納法来証明引理. 由于

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^2=\sum_{x=0}^{P} e^{-2\pi i f(x)\alpha}\sum_{-x\leqslant h\leqslant P-x} e^{2\pi i f(x+h)\alpha}=$$
$$=\sum_{|h|\leqslant P}{}'\sum_{x=1}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha},$$

此处 $\sum'$ 表示經过所示区間內整数的某一部分集合,而

$$\varphi(x,h)=\begin{cases}\dfrac{1}{h}(f(x+h)-f(x)), & 若\ h\neq 0;\\ 0, & 若\ h=0,\end{cases}$$

故由 Hölder 不等式可知

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2\cdot 8^{k-2}} \ll P^{8^{k-2}-1}\sum_{|h|\leqslant P}{}'\left|\sum_{x=1}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha}\right|^{8^{k-2}}=$$
$$=P^{8^{k-2}-1}\sum_{|h|\leqslant P}{}'\sum_{n} r(n)e^{2\pi i h n\alpha}, \tag{5}$$

此处

$$r(n)=\int_0^1\left|\sum_{x=0}^{P}{}' e^{2\pi i\varphi(x,h)\beta}\right|^{8^{k-2}} e^{-2\pi i n\beta}d\beta. \tag{6}$$

由归納法假定可知 $r(n)\ll P^{8^{k-2}-(k-1)}$. 所以由(3),再将(5)式四方,并从 0 至 1 求积分,便得

$$\int_0^1\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll$$
$$\ll P^{4(8^{k-2}-1)}\int_0^1\left|\sum_{|h|\leqslant P}{}'\sum_{n} r(n)e^{2\pi i h n\alpha}\right|^4 d\alpha \ll$$
$$\ll P^{4(8^{k-2}-1)}\sum_{hn+h'n'=h''n''+h'''n'''} r(n)r(n')r(n'')r(n''')\ll$$
$$\ll P^{4(8^{k-2}-1)+4(8^{k-2}-(k-1))+3(k-1+1)}=$$
$$=P^{8^{k-1}-k}.$$

取 $\mathfrak{A}_t^*$ 为整数

$$x_1^k+\cdots+x_t^k$$

所成之集合，此处 x_m 各自經过全体非負整数. 定义 $\mathfrak{A}_t$ 为 $\mathfrak{A}_t^*$ 中的不同元素所成之最大子集. 命 $c_1=\frac{1}{2}8^{k-1}$ 及 $r(a)$ 为不定方程

$$x_1^k+\cdots+x_{c_1}^k=a,\quad x_m\geqslant 0$$

的解数,则显然

$$\sum_{1\leqslant a\leqslant n} r(a)\gg\left(\frac{n}{c_1}\right)^{\frac{c_1}{k}}\gg n^{\frac{c_1}{k}}.$$

又由(4)可知

$$\sum_{1\leqslant a\leqslant n} r^2(a)\ll n^{\frac{2c_1}{k}-1},$$

故由定理(D)可知,当 $k\geqslant 2$ 时,集合 $\mathfrak{A}_{c_1}$ 有正密率. 因此我們証明了

Hilbert-Waring 定理. 对于任意整数 $k\geqslant 2$, 恆存在一仅依賴于 k 的整数 $s=s(k)$, 使每一正整数都是不超过 s 个正整数的 k 次方之和.

3. 篩法及 Шнирельман-Гольдбах定理

Möbius 函数 $\mu(n)$ 是正整数 n 的函数, 其定义如下: $\mu(1)=1$; 若 n 能被一素数的平方所整除,则 $\mu(n)=0$;又若 n 为 r 个不同素数之乘积,则 $\mu(n)=(-1)^r$.

古典的 Eratosthenes 篩法可以用下面的方式陈述出来: 命 P 为 $\leqslant\xi$ 的全体素数的乘积,则

$$\sum_{d|(P,n)}\mu(d)=\begin{cases}1, & \text{若 } n \text{ 无} \leqslant\xi \text{ 的素因子;}\\ 0, & \text{其他情形.}\end{cases}\tag{7}$$

命 $\mathfrak{B}$ 为由 M 个相同或相异的整数 b 所成之集合, N_ξ 为 $\mathfrak{B}$中不能被 $\leqslant\xi$ 的素数整除的元素 b 的个数,则得

$$N_\xi=\sum_b\Big(\sum_{d|(P,b)}\mu(d)\Big).\tag{8}$$

交換(8)中的求和次序,便得

$$N_\xi=\sum_{d|P}\mu(d)\sum_{d|b}1=\sum_{P|P}\mu(d)N(d),\tag{9}$$

此处 $N_d=\sum_{d|b}1$ 为 $\mathfrak{B}$ 中能被 d 整除的元素 b 的个数.

用 Eratosthenes 原来的形式, 可以将(9)式叙述为: 先減掉集合 $\mathfrak{B}$ 中为 2, 3, 5, $\cdots$ (素数貫)倍数的元素的个数. 假如一个数为两个素数的乘积所整除, 因为它被

計算了两次,所以需要添上 $\mathfrak{B}$ 中为 $2\cdot 3, 2\cdot 5, 3\cdot 5, \cdots$(两个素数乘积的貫)的倍数的元素的个数. 又因为被三个素数的乘积整除的元素,共計算了 $\binom{3}{1}-\binom{3}{2}=0$ 次,所以又需减掉 $\mathfrak{B}$ 中为 $2\cdot 3\cdot 5, \cdots$(三个素数乘积的貫)整除的元素的个数. 如此等等.

若 $N(d)$ 有渐近表达式

$$N(d)=g(d)\frac{N}{d}+R_d, \tag{10}$$

此处 $g(d)$ 为无平方因子数的积性函数. 則由(9)得

$$N_\xi=\sum_{d\mid P}\frac{\mu(d)}{d}g(d)N+O\left(\sum_{d\mid P}|R_d|\right)=$$

$$=N\prod_{p\mid P}\left(1-\frac{g(p)}{p}\right)+O\left(\sum_{d\mid P}|R_d|\right). \tag{11}$$

除了一些很显然的情况外,(11)的余項常常比主項更大,因此(11)几乎是无用的.

Brun[14] 对篩法作了重大的改进. 命

$$2=p_1<p_2<\cdots<p_{k_0}\leqslant\xi$$

为 $\leqslant\xi$ 的全体素数,又

$$k_0\geqslant k_1\geqslant\cdots\geqslant k_{t-1}\geqslant 1$$

为一整数集合. 命 Q 为具有如下形式的整数的集合:

$$d=1;\quad d=p_{r_1}p_{r_2}\cdots p_{r_s},\quad s\leqslant 2t, \tag{12}$$

其中 $r_1>r_2>\cdots>r_s$, $r_j\leqslant k_{\left[\frac{j-1}{2}\right]}$, $1\leqslant j\leqslant s$. 則得

$$\sum_{\substack{d\mid n\\ d\in Q}}\mu(d)\begin{cases}=1, & \text{若 } n \text{ 无} \leqslant\xi \text{ 的素因子;}\\ \geqslant 0, & \text{其他情形.}\end{cases} \tag{13}$$

事实上,若 n 无 $\leqslant\xi$ 的素因子,則(13)式显然成立. 若 n 有 $\leqslant\xi$ 的素因子,則以 p_0 表示 n 的最小素因子. 当 $d\in Q$, $d\mid n$ 及 d 的素因子个数为奇数时,我們就定义 d_1 如下:若 $p_0\mid d$,則 $d_1=\frac{d}{p_0}$; 若 $p_0\nmid d$,則 $d_1=dp_0$. 因此 $d_1\mid n$, $d_1\in Q$ 且 d_1 的素因子个数为偶数. 由于每一个 d 都唯一地对应到一个 d_1,故得(13).

由(13)可知

$$N_\xi\leqslant\sum_b\sum_{\substack{d\in Q\\ d\mid(b,P)}}\mu(d)=\sum_{d\in Q}\mu(d)\sum_{d\mid b}1=$$

$$=N\sum_{d\in Q}\mu(d)\frac{g(d)}{d}+O\left(\sum_{d\in Q}|R_d|\right). \tag{14}$$

对于各种間題,我們选取适当的 $k_0, \cdots, k_{t-1}$,就能得到 N_ξ 的上界.

其次,我們用另一集合 Q' 来代替集合 Q. 命 $k_0 \geqslant k_1 \geqslant \cdots \geqslant k_t \geqslant 1$, Q' 为适合下面条件的整数集合:

$$d'=1, \quad d'=p_{r_1}p_{r_2}\cdots p_{r_s}, \quad s \leqslant 2t+1,$$

其中 $r_1 > r_2 > \cdots > r_s$ 及 $r_i \leqslant k_{[\frac{1}{2}i]}$. 对应于(13),有

$$\sum_{\substack{d'|n \\ d' \in Q'}} \mu(d') \begin{cases} =1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子;} \\ \leqslant 0, & \text{其他情形.} \end{cases}$$

类似地,我們得到 N_ξ 的下界如下:

$$N_\xi \geqslant N \sum_{d' \in Q'} \frac{\mu(d')g(d')}{d'} + O\left(\sum_{d' \in Q'} |R_{d'}|\right). \tag{15}$$

取 $\mathfrak{B}$ 为整数

$$x(a-x), \quad 1 \leqslant x \leqslant a$$

的集合. 再适当地选取(14)中的 $k_i (1 \leqslant i \leqslant t-1)$. Шнирельман 証明了下面的結果:命 $r(a)$ 为方程 $a = p_1 + p_2$ 的解数,此处 p_1, p_2 为素数,则

$$r(a) \ll \frac{a}{\log^2 a} \sum_{k|a} \frac{\mu^2(k)}{k}. \tag{16}$$

与 §1 相同的記号. 取 $\mathfrak{A}^*$ 为由整数 1 及諸整数 $a = p_1 + p_2 (1 < p_1, p_2 \leqslant a)$ 所成的集合,则显然有

$$\sum_{1 \leqslant a \leqslant n} r(a) = 1 + \sum_{p_1 + p_2 \leqslant n} 1 \geqslant \left(\sum_{p_1 \leqslant \frac{n}{2}} 1\right)^2 \gg \left(\frac{n}{\log n}\right)^2.$$

又因 d 与 d' 的最小公倍数 $\{d_1, d_2\} \geqslant (dd')^{\frac{1}{2}}$,故由(16)得到

$$\begin{aligned}\sum_{1 \leqslant a \leqslant n} r^2(a) &\ll \sum_{4 \leqslant a \leqslant n} \frac{a^2}{\log^4 a} \sum_{d|a} \frac{1}{d} \sum_{d'|a} \frac{1}{d'} \ll \\ &\ll \frac{n^2}{\log^4 n} \sum_{d, d' \leqslant n} \frac{1}{dd'} \sum_{\substack{1 \leqslant a \leqslant n \\ d|a,\ d'|a}} 1 \ll \\ &\ll \frac{n^3}{\log^4 n} \left(\sum_{1 \leqslant d \leqslant n} \frac{1}{d^{3/2}}\right)^2 \ll \frac{n^3}{\log^4 n}.\end{aligned}$$

于是由 §1, 定理(D)可知, 由 1 及可以表为两个素数之和的諸整数所成的集合具有正密率. 因此由定理(C),我們得到下面的享有盛名的定理.

Шнирельман-Гольдбах 定理. 存在整数 c, 使每一整数都是不超过 c 个素数之和.

命 s 表示最小的整数, 使每一充分大的整数都能表成不多于 s 个素数之和.

Шнирельман的方法不仅証明了 s 的存在性，而且可以得到 s 的明确上界。他的方法給出 $s \leqslant 800,000$。Романов[41] 又在以后証明了 $s \leqslant 2208$。沿着这一方向，还有如下更进一步的改进：Heilbronn，Landau 与 Scherk[42] 得到 $s \leqslant 71$，而估計 $s \leqslant 67$ 則是属于 Ricci[43] 的。

在(15)中选取适当的 $k_0, k_1, \cdots$，Brun 首先証明了：每一充分大的偶数都是两个各不超过 9 个素数的乘积之和。Rademacher[44] 将 9 改进为 7，而 Estermann[45] 又将 7 减至 6。

Бухштаб[46] 成功地以 4 代替了 6，他改进这一結果的主要想法如下：命

$$3 = p_1 < p_2 < \cdots < p_k$$

为不超过 y 的全体素数。又命

$$(w) \qquad a;\ a_1,\ b_1;\ a_2,\ b_2;\ \cdots;\ a_k,\ b_k$$

为适合下面条件的整数集合：

$$a = 0 \text{ 或 } 1,\ a_i \neq b_i,\ 0 \leqslant a_i,\ b_i < p_i,\ 1 \leqslant i \leqslant k;$$

而命 $F_w(x, y)$ 为适合下面条件的整数 n 的个数：

$$1 \leqslant n \leqslant x;\ n \equiv a(\bmod 2),\ n \not\equiv a_i(\bmod p_i),\ n \not\equiv b_i(\bmod p_i),$$
$$(1 \leqslant i \leqslant k)$$

則得

$$F_w(x; p_s) = F_w(x; p_{s-1}) - F_{w_s'}\left(\frac{x}{p_s};\ p_{s-1}\right) - F_{w_s''}\left(\frac{x}{p_s};\ p_{s-1}\right) + 2\theta,$$
$$0 \leqslant |\theta| \leqslant 1. \tag{17}$$

命 $v > u \geqslant 2$。将 $x^{\frac{1}{v}}$ 与 $x^{\frac{1}{u}}$ 之間的素数依次排列为 $p_t \leqslant x^{\frac{1}{v}} < p_{t+1} < \cdots < p_k \leqslant$ $\leqslant x^{\frac{1}{u}} < p_{k+1}$，則連續运用(17)便得

$$F_w(x; x^{\frac{1}{u}}) = F_w(x; x^{\frac{1}{v}}) - \sum_{i=t+1}^{k} F_{w_i'}\left(\frac{x}{p_i};\ p_{i-1}\right) -$$
$$- \sum_{i=t+1}^{k} F_{w_i''}\left(\frac{x}{p_i};\ p_{i-1}\right) + 2k\theta. \tag{18}$$

Бухштаб 用 Brun 方法証明了：存在两个非負的阶梯函数 $\lambda(u)$ 及 $\Lambda(u)$，使当 x 充分大时，下式对于 w 一致地成立：

$$\lambda(u)\frac{cx}{\log^2 x} \leqslant F_w(x;\ x^{\frac{1}{u}}) \leqslant \Lambda(u)\frac{cx}{\log^2 x}, \quad 15 \geqslant u \geqslant 2. \tag{19}$$

由(18)，我們可以构造两个阶梯函数

$$\lambda_1(u) \leqslant \lambda(v) - 2\int_{u-1}^{v-1} \Lambda(z)\,\frac{z+1}{z^2}\,dz$$

及

$$\Lambda_1(u) \geqslant \Lambda(v) - 2\int_{u-1}^{v-1} \lambda(z)\,\frac{z+1}{z^2}\,dz.$$

它們分别具有与 $\lambda(u)$ 及 $\Lambda(u)$ 相同的性質. 进而言之,我們有

$$\lambda(u) \leqslant \lambda_1(u) \leqslant g(u) \leqslant \Lambda_1(u) \leqslant \Lambda(u).$$

不断运用这个原则,并經过一些复杂的計算,就能得到 Бухштаб 的結果.

4. 續

Selberg[15)17)47)] 对篩法作出了另一重要的改进.

命 $\lambda_1, \lambda_2, \cdots$ 为一实数貫,它满足 $\lambda_1 = 1$, 且当 $d > \sqrt{z}$ 时, $\lambda_d = 0$. 則显然有

$$\Big(\sum_{d|(n,P)} \lambda_d\Big)^2 \begin{cases} = 1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子;} \\ \geqslant 0, & \text{其他情形,} \end{cases}$$

此处 $P = \prod_{p \leqslant \xi} p$. 因此

$$\begin{aligned} N_\xi &= \sum_b \Big(\sum_{d|(b,P)} \mu(d)\Big) \leqslant \sum_b \Big(\sum_{d|(b,P)} \lambda_d\Big)^2 = \\ &= \sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} \sum_{\substack{b \\ \{d,d'\}|b}} 1 = \\ &= N \sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} \frac{g(\{d,d'\})}{\{d,d'\}} + \sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} R_{\{d,d'\}}, \end{aligned}$$

此处 $\{d, d'\}$ 表示 d 与 d' 的最小公倍. Selberg 定出了使二次型

$$\sum_{\substack{d \leqslant \sqrt{z} \\ d|P}} \sum_{\substack{d' \leqslant \sqrt{z} \\ d'|P}} \lambda_d \lambda_{d'} \frac{g(\{d,d'\})}{\{d,d'\}}$$

取极小値的諸 λ,从而得到了 N_ξ 的上界.

为了估計 N_ξ 的下界,我們假定 $\lambda_1 = 1$. 若 $p \leqslant \xi$,則 $\lambda_p = 1$; 若 $d > \sqrt{\frac{z}{p}}$, 則 $\lambda_{d\cdot p} = 0$. 易知

$$1 - \sum_{p|(n,P)} \Big\{\sum_{\substack{d|(n,P) \\ p'|d \Rightarrow p' < p}} \lambda_{d\cdot p}\Big\}^2 \begin{cases} = 1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子;} \\ \leqslant 0, & \text{其他情形.} \end{cases}$$

故得

$$N_\xi \geqslant \sum_b \Big(1 - \sum_{p|(b,P)} \Big\{ \sum_{\substack{d|(b,P) \\ p'|d \Rightarrow p'<p}} \lambda_{d\cdot p} \Big\}^2 \Big) =$$

$$= N - \sum_{p\leqslant\xi} \sum_{\substack{d\leqslant\sqrt{\frac{z}{p}} \\ p'|d\Rightarrow p'<p \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{\frac{z}{p}} \\ p'|d'\Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p}\lambda_{d'\cdot p} \sum_{\substack{b \\ p\{d,d'\}|b}} 1 =$$

$$= N\Big(1 - \sum_{p\leqslant\xi} \frac{g(p)}{p} \sum_{\substack{d\leqslant\sqrt{\frac{z}{p}} \\ p'|d\Rightarrow p'<p \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{\frac{z}{p}} \\ p'|d'\Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p}\lambda_{d'\cdot p} \frac{g(\{d,d'\})}{\{d,d'\}}\Big) -$$

$$- \sum_{p\leqslant\xi} \sum_{\substack{d\leqslant\sqrt{\frac{z}{p}} \\ p'|d\Rightarrow p'<p \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{\frac{z}{p}} \\ p'|d'\Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p}\lambda_{d'\cdot p} R_{p\cdot\{d,d'\}}.$$

定出諸 λ,使表达式

$$1 - \sum_{p\leqslant\xi} \frac{g(p)}{p} \sum_{\substack{d\leqslant\sqrt{\frac{z}{p}} \\ p'|d\Rightarrow p'<p \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{\frac{z}{p}} \\ p'|d'\Rightarrow p'<p \\ d'|P}} \lambda_{d\cdot p}\lambda_{d'\cdot p} R_{p\cdot\{d,d'\}}$$

取极大値. 我們便得到 N_ξ 的下界.

就已知的各种情况而言, Selberg 方法都比 Brun 方法精密. 例如, Shapiro 与 Warga[48] 用 Selberg 方法証明了:每一充分大的自然数都是不超过 20 个素数之和. 尹文霖[49] 在应用了漸近密率的两个結果之后,証明了:每一充分大的奇数都可表成不超过 17 个素数之和.

Eratosthenes–Brun–Selberg 篩法还可以用到許多其他問題上去. 我們現在列举一下这些問題的最近記录.

区間 $(A, A+N)$ 中的素数的个数 $\leqslant 2\frac{N}{\log N} + O\Big(\frac{N}{\log^2 N}\log\log N\Big)$,此处与 O 有关的常数与 A 无关(Selberg[47]).

不超过 N 的孿生素数对 $(p, p+2)$ $(p<N)$ 的对数 $\leqslant 16\prod_{p>2}\Big(1-\frac{1}{(p-2)^2}\Big)\frac{N}{\log^2 N} + O\Big(\frac{N}{\log^3 N}\log\log N\Big)$ (Selberg[47]).

固定常数 $0<\delta<1$, 则在算术級数 $kn+l$ $(n=1, 2, \cdots)$ 中不超过 x 的素数的个数

$$\leqslant \frac{2x}{\varphi(k)\log\frac{x}{k}} + O\Big(\frac{x}{\log^2 x}\log\log x\Big),$$

此处与 O 有关的常数对于适合 $k \leqslant x^{\delta}$ 的 k 都是一致的(Чулановский[50]).

若 $F(x)$ 为无固定素因子的既約 k 次整值多項式,則当 $x = 1, 2, \cdots, N$ 时,使 $F(x)$ 为素数的 x 的个数 $\leqslant 2e^{\gamma}\mu_F \frac{N}{\log N} + o\left(\frac{N}{\log N}\right)$,此处 γ 为 Euler 常数,而 μ_F 及与 o 有关的常数都是只依賴于 $F(x)$ 的常数(王元[51]).

命 l 为适合不等式

$$\log \frac{5(6k-l)}{l+6} \leqslant 1.097(l+1)$$

的最小整数. Kuhn[52] 証明了:存在无穷多个整数 x,使 $F(x)$ 为不超过 $l+k$ 个素数的乘积.

关于以上問題的过去发展情况,請参看 Ricci[43,53] 及 Heilbronn[54] 的文章.

王元[55] 綜合运用了 Бухштаб 方法与 Selberg 方法,从而証明了每一充分大的偶数都是一个不超过 3 个素数的乘积及一个不超过 4 个素数的乘积之和. А. И. Виноградов[16] 在运用了 Riemann ζ-函数的某些性质之后,証明了每一充分大的偶数都是两个素因子个数各不超过 3 的整数之和.

在广义 Riemann 猜想之下,王元[56] 証明了每一充分大的偶数都是一个素数及一个素因子个数不超过 4 的整数之和. 同样亦証明了存在无穷多个素数 p,使 $p+2$ 为不超过 4 个素数的乘积.

5. 素数定理的初等証明

是否可以不用复变函数論的理論来証明素数定理[57],这对于数学家来說,是一个长期悬而未决的問題. 命 $\pi(x)$ 表示不超过 x 的素数的个数,所謂素数定理,就是

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1. \tag{20}$$

不久以前,Selberg[58] 与 Erdös[59] 才找到了一个适合上面要求的証明.

大家知道,我們可以不用复变函数論的理論来証明下面这些結果:

a)

$$0 < c_1 < \frac{\pi(x)}{\frac{x}{\log x}} < c_2, \quad x \geqslant 2; \tag{21}$$

b) (20)等价于

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1, \tag{22}$$

此处 $\theta(x)=\sum_{p\leqslant x}\log p$;

c)

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

以上都是 Чебышев 的結果.

Selberg 証明的起点就是他的著名恆等式:

$$\theta(\xi)\log\xi+\sum_{p\leqslant\xi}\theta\left(\frac{\xi}{p}\right)\log p=2\xi\log\xi+O(\xi). \tag{23}$$

这是下面广义的 Möbius 反轉公式的推論:方程

$$G(x)=\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\log x \tag{24}$$

等价于

$$\sum_{n\leqslant x}\mu(n)G\left(\frac{x}{n}\right)=F(x)\log x+\sum_{n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n), \tag{25}$$

此处当 n 为素数 p 的方幂时, $\Lambda(n)=\log p$,否則 $\Lambda(n)=0$. 置 $F(x)=\sum_{n\leqslant x}\Lambda(n)-$ $-x+\gamma+1$ (γ 为 Euler 常数), 則由(24)可知 $G(x)=O(\log^2 x)$. 故由(25)可得(23)(Tatuzawa 与 Iseki[60]).

素数定理是(23)及下面这条与数論无关的定理的推論:

命 $K(x)$ 为非負递減函数,

$$g(x)=\int_0^x e^u dK(u). \tag{26}$$

若当 $x\to\infty$ 时,有

$$0<c_1<g(x)e^{-x}<c_2,\quad K(x)\sim x \tag{27}$$

及

$$g(x)+\frac{1}{x}\int_0^x g(x-u)\,dg(u)\sim 2e^x, \tag{28}$$

則当 $x\to\infty$ 时,

$$g(x)\sim e^x. \tag{29}$$

取 $K(u)=\sum_{p\leqslant e^u}\frac{\log p}{p}$, 則 $g(x)=\theta(e^x)=\sum_{p\leqslant e^x}\log p$. 关系(27)就是 Чебышев 定理, 而結論(29)就是素数定理. 素数定理的証明虽然是初等的, 但却是十分复杂的.

Selberg 的初等方法还可以用来証明很多以往曾用解析方法得到的結果. 現在我們列举这些結果及其作者.

命 $\pi(x;\, q,\, l)$ 表示不超过 x 且 $\equiv l \pmod q$ 的素数的个数. 若 $(q,\, l)=1$,则

$$\pi(x;\, q,\, l) \sim \frac{x}{\varphi(q)\log x} \quad \text{(Selberg[61], Shapiro[62])}.$$

每一个二次原型 $ax^2+2bxy+cy^2$ $(a>0,\ D=b^2-ac$ 非平方数)可以表出无穷多个素数(Briggs[63]).

命 K 为一代数数域, $N\mathfrak{p}$ 表示素理想数 $\mathfrak{p}$ 的矩,则

$$\pi_K(x)=\sum_{N\mathfrak{p}\leqslant x} 1 \sim \frac{x}{\log\ x} \quad \text{(Shapiro[64])}. \tag{30}$$

Forman 与 Shapiro[65] 还証明了一个抽象素数定理,不少素数定理都是它的特殊情形.

6. 几何数論的初等方法

命 $A(x)$ 表示圓 $u^2+v^2\leqslant x$ 內整点 $(u,\, v)$ 的个数. Gauss 的"圓問題"就是去寻求最小的 ϑ,使

$$A(x)=\pi x+O(x^{\vartheta+\varepsilon})$$

对所有的 $\varepsilon>0$ 都成立. 类似地,命 $D(x)$ 表示双曲綫 $uv\leqslant x,\ u>0,\ v>0$ 內整点 $(u,\, v)$ 的个数. Dirichlet 的"除数問題"就是去寻求最小的 ϑ,使

$$D(x)=x\log x+(2\gamma-1)x+O(x^{\vartheta+\varepsilon})$$

对所有的 $\varepsilon>0$ 都成立,此处 γ 为 Euler 常数. 迄今为止,这两个問題都还沒有解决. Gauss[66] 与 Dirichlet[67] 曾証明过 $\vartheta\leqslant\frac{1}{2}$. 这里我們将概述一下 Виноградов[68] 关于 $\vartheta\leqslant\frac{1}{3}$ 的初等証明.

引. 命 m 为整数, $A>2,\ k\geqslant 1$,

$$S=\sum_{x=M}^{M+m-1}\{f(x)\},$$

此处 $f(x)$ 在区間 $M\leqslant x\leqslant M+m-1$ 中定义,它有二阶导数,且适合

$$\frac{1}{A}\leqslant |f''(x)|\leqslant\frac{k}{A},$$

则

$$S-\frac{1}{2}m \ll (k^2 m\log A+kA)A^{-\frac{1}{3}}.$$

証. 命 $\tau=A^{\frac{1}{3}}$. 我們按照 $f'(x)$ 将求和区間分成若干子区間. 取 $M_1=M$,则有一对整数 $(a_1,\, m_1)$ 满足

$$\left|f'(M_1)-\frac{a_1}{m_1}\right|\leqslant\frac{1}{m_1\tau},\quad 0<m_1\leqslant\tau,\quad (a_1, m_1)=1.$$

命 S_1 表示分和

$$S_1=\sum_{x=M_1}^{M_1+m_1-1}\{f(x)\}.$$

其次，置 $M_2=M_1+m_1$，則有一对整数 (a_2, m_2) 滿足

$$\left|f'(M_2)-\frac{a_2}{m_2}\right|\leqslant\frac{1}{m_2\tau},\quad 0<m_2\leqslant\tau,\quad (a_2, m_2)=1.$$

再命

$$S_2=\sum_{x=M_2}^{M_2+m_2-1}\{f(x)\}.$$

进而言之，取 $M_3=M_2+m_2$，如此等等。 假定經过 s 步后得到

$$0\leqslant M+m-1-M_{s+1}<\tau,$$

則得

$$|S-S_1-\cdots-S_s|\leqslant\tau+1.$$

引理的証明可以分成两步：第一，估計每一分和，得

$$\left|S_\nu-\frac{1}{2}m_\nu\right|\leqslant\frac{1}{2}(k+5);$$

第二，証明步数 $s\ll\frac{km}{\tau}\log A+\frac{A}{\tau}$. 引理証完。

在圓問題上的应用. 显然

$$A(x)=1+4[\sqrt{x}]+8\sum_{0<u\leqslant\sqrt{\frac{x}{2}}}[\sqrt{x-u^2}]-4\left[\sqrt{\frac{1}{2}x}\right]^2.$$

命

$$\sum_{0<u\leqslant\sqrt{\frac{x}{2}}}[\sqrt{x-u^2}]=\sum_{0<u\leqslant\sqrt{\frac{x}{2}}}\sqrt{x-u^2}-\sum_{0<u\leqslant\sqrt{\frac{x}{2}}}\{\sqrt{x-u^2}\}=\Sigma_1-\Sigma_2.$$

由 Euler 求和公式得到

$$\Sigma_1=\frac{\pi}{8}x+\frac{x}{4}+\left(\frac{1}{2}-\left\{\sqrt{\frac{x}{2}}\right\}\right)\sqrt{\frac{x}{2}}-\frac{1}{2}\sqrt{x}+O(1).$$

又由引理可知

$$\Sigma_2=\frac{1}{2}\sqrt{\frac{x}{2}}+O(x^{\frac{1}{3}}\log x),$$

因此

$$A(x)=\pi x+O(x^{\frac{1}{3}}\log x).$$

在除数問題上的应用. 显然

$$D(x) = \sum_{1 \leqslant uv \leqslant x} 1 = 2 \sum_{1 \leqslant u \leqslant \sqrt{x}} \left[\frac{x}{u}\right] - [\sqrt{x}]^2.$$

由 Euler 求和公式可知

$$2 \sum_{1 \leqslant u \leqslant \sqrt{x}} \frac{x}{u} = x \log x + 2\left(\frac{1}{2} - \{\sqrt{x}\}\right) x^{\frac{1}{2}} + 2\gamma x + O(1).$$

命 t_0 为适合 $[\sqrt{x}]2^{-t_0} \geqslant 2x^{\frac{1}{3}} \geqslant [\sqrt{x}]2^{-t_0-1}$ 的整数，則由引理可知

$$\sum_{1 \leqslant u \leqslant \sqrt{x}} \left\{\frac{x}{u}\right\} = \sum_{t=0}^{t_0} \sum_{[\sqrt{x}]2^{-t-1} \leqslant u \leqslant [\sqrt{x}]2^{-t}} \left\{\frac{x}{u}\right\} + O(x^{\frac{1}{3}}) =$$

$$= \sum_{t=0}^{t_0} \left(\frac{1}{2^{t+2}}[\sqrt{x}] + O(x^{\frac{1}{3}} \log x)\right) + O(x^{\frac{1}{3}}) =$$

$$= \frac{1}{2}[\sqrt{x}] + O(x^{\frac{1}{3}} \log^2 x).$$

故得

$$D(x) = x \log x + (2\gamma - 1)x + O(x^{\frac{1}{3}} \log^2 x).$$

附注. Jarnik[69] 推广了 Gauss 原来的方法，从而証明了：命 D 为一 Jordan 域，其面积为 A，而周长为 L，則 D 中的整点个数 N 适合

$$|N - A| < L.$$

第二章　指数和的估計

7. Weyl 方 法

Weyl 在他关于一致分布的开創性工作中，首先引进了一个給予指数和以非无聊估計的方法．这个方法基于不等式

$$\left|\sum_{x=a+1}^{a+P} e^{2\pi i \alpha x}\right| \leqslant \min\left(P, \frac{1}{|\sin \pi\alpha|}\right) \tag{31}$$

及下面的引理：

引． 命 $k \geqslant 1$，又命 $f(x)$ 为实函数及

$$\mathop{\Delta}_{y} Q(x) = \frac{1}{y}(Q(x+y) - Q(x)), \quad I = \sum_{x=1}^{P} e^{2\pi i f(x)}.$$

我們用記号 $\sum_{x}^{P\,'}$ 来表示在有限多个区間上的求和，而这些区間的长度之和 $\ll P$．于是当 $1 \leqslant \mu \leqslant k$ 时，有

$$|I|^{2^\mu} \ll P^{2^\mu-\mu-1} \sum_{y_1}^{P} \cdots \sum_{y_\mu}^{P} \sum_{x_{\mu+1}}^{P}{}' e^{2\pi i (y_1 \cdots y_\mu \mathop{\Delta}_{y_\mu} \cdots \mathop{\Delta}_{y_1} f(x_{\mu+1}))}, \tag{32}$$

此处与 $\ll$ 有关的常数仅依賴于 μ．

易知，当 $\mu = 1$ 时引理成立．由归納法及 Буняковский-Schwarz 不等式得到

$$|I|^{2^\mu} = |I^{2^{\mu-1}}|^2 \ll P^{2(2^{\mu-1}-\mu)} \left|\sum_{y_1}^{P} \cdots \sum_{y_{\mu-1}}^{P} \sum_{x_\mu}^{P}{}' e^{2\pi i (y_1 \cdots y_{\mu-1} \mathop{\Delta}_{y_{\mu-1}} \cdots \mathop{\Delta}_{y_1} f(x_\mu))}\right|^2 \ll$$

$$\ll P^{2^\mu-\mu-1} \sum_{y_1}^{P} \cdots \sum_{y_{\mu-1}}^{P} \left|\sum_{x_\mu}^{P}{}' e^{2\pi i (y_1 \cdots y_{\mu-1} \mathop{\Delta}_{y_{\mu-1}} \cdots \mathop{\Delta}_{y_1} f(x_\mu))}\right|^2,$$

故得(32)．

取 $f(x)$ 为 $k\,(>1)$ 次多項式，$f(x) = \alpha x^k + \cdots$，則由(31)及(32)(取 $\mu = k-1$)得

$$\left|\sum_{x=a+1}^{a+P} e^{2\pi i f(x)}\right|^{2^{k-1}} \ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{y_1}^{P} \cdots \sum_{y_{k-1}}^{P}{}^{*} \left|\sum_{x_k}^{P}{}' e^{2\pi i k!\, y_1 \cdots y_{k-1} \alpha x_k}\right| \ll$$

$$\ll P^{2^{k-1}-1} + P^{2^{k-1}-k} \sum_{y_1, \cdots, y_{k-1}}^{P}{}^{*} \min\left(P, \frac{1}{\{k!\, y_1 \cdots y_{k-1}\alpha\}}\right), \tag{33}$$

此处 * 表示条件 $y_1\cdots y_{k-1}\neq 0$,而

$$\{\beta\}=\min(\beta-[\beta],\quad[\beta]+1-\beta).$$

由除数函数的性質可知,对于任意 $\varepsilon>0$, $Y=k!\,y_1\cdots y_{k-1}$ 的解答 $y_1,\cdots,y_{k-1}$ 的組数为 $O(Y^{\varepsilon})$. 所以

$$\left|\sum_{x=a+1}^{a+P}e^{2\pi if(x)}\right|^{2^{k-1}}\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{0<Y\ll P^{k-1}}\min\left(P,\frac{1}{\{Y\alpha\}}\right).\qquad(34)$$

不等式(34)有着广泛的应用:

例 1. 若 α 充分小,例如 $\alpha=o(P^{-(k-1)})$,則

$$\left|\sum_{x=a+1}^{a+P}e^{2\pi if(x)}\right|^{2^{k-1}}\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{Y}\min\left(P,\frac{1}{\{Y\alpha\}}\right)\ll$$

$$\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+\varepsilon}\sum_{Y}\frac{1}{Y|\alpha|}\ll$$

$$\ll P^{2^{k-1}-1}+P^{2^{k-1}-k+2\varepsilon}\frac{1}{|\alpha|}.$$

卽对 $\varepsilon>0$,

$$\sum_{x=a+1}^{a+P}e^{2\pi if(x)}\ll P^{1-2^{1-k}}+P^{1-k\cdot2^{1-k}+\varepsilon}|\alpha|^{-2^{1-k}}.$$

例 2. 若 $\alpha_k,\cdots,\alpha_0$ 皆为实数,而且

$$f(x)=\alpha_kx^k+\cdots+\alpha_1x+\alpha_0,\quad\left|\alpha_k-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad(h,q)=1,$$

則

$$\sum_{x=1}^{P}e^{2\pi if(x)}\ll P^{1+\varepsilon}q^{\varepsilon}\left(\frac{1}{P}+\frac{1}{q}+\frac{q}{P^k}\right)^{2^{1-k}}.$$

証明依賴于下面的不等式:

$$\sum_{Y}^{P^{k-1}}\min\left(P,\frac{1}{\{Y\alpha_k\}}\right)\ll\left(\frac{P^{k-1}}{q}+1\right)\max_{f}\left(\sum_{Y=f+1}^{f+q}\min\left(P,\frac{1}{\{Y\alpha_k\}}\right)\right)\ll$$

$$\ll\left(\frac{P^{k-1}}{q}+1\right)(P+q\log q).$$

8. Van der Corput 方法

如果分析一下上节的方法,我們就会发現这个方法的两个重要步驟为: 1) 运用 $k-1$ 次 Буняковский-Schwarz 不等式,及 2) 直接处理 $k=1$ 的情形. 由于 Буняковский-Schwarz 不等式用得愈多,估計愈坏,所以这就建議了这样一种做法: 1) 直接处理 $k=2$ 的情形, 及 2) 运用 $k-2$ 次 Буняковский-Schwarz 不等式. 下面的

Hardy-Littlewood[70] 定理指出了这是可能的.

命 $\vartheta > 0$, ϑ_1 为实数及 $A < B$,则

$$\left| \sum_{x=A}^{B}{}' e^{2\pi i(\vartheta x^2+2\vartheta_1 x)} - \frac{e^{\frac{\pi i}{4}}}{\sqrt{\vartheta}} \sum_{x=A\vartheta+\vartheta_1}^{B\vartheta+\vartheta_1} e^{-\frac{\pi i}{\vartheta}(x-\vartheta_1)^2} \right| < \frac{1}{2}\left(1+\frac{1}{\sqrt{\vartheta}}\right), \tag{35}$$

此处 $\sum_{x=A}^{B}{}'$ 表示项 $x = A$ 及 $x = B$ 仅取其值之半.

由此可見,

$$\sum_{x=A}^{B}{}' e^{2\pi i\left(\frac{\vartheta}{2}x^2+\vartheta_1 x\right)} \ll (B-A)|\vartheta|^{\frac{1}{2}} + |\vartheta|^{-\frac{1}{2}}. \tag{36}$$

这由 van der Corput[34] 成功地将它变为下面的定理.

定理 1. 若 $f(x)$ 为实函数,它在区間 (a, b) 中有二阶导数,并且适合

$$0 < r < f''(x) \leqslant hr \quad (\text{或 } 0 < r \leqslant -f''(x) \leqslant hr),$$

此处 $b \geqslant a+1$, 则

$$\sum_{a<n\leqslant b} e^{2\pi i f(n)} \ll h(b-a)r^{\frac{1}{2}} + r^{-\frac{1}{2}}.$$

下面的引理是一个与定理 1 类似的积分估計.

引 1. 命 $f(x)$ 为实函数,它在区間 (a, b) 中有二阶导数,并且适合 $f''(x) \geqslant r > 0$ (或 $f''(x) \leqslant -r < 0$),则

$$\left| \int_a^b e^{if(x)}dx \right| \leqslant \frac{8}{\sqrt{r}}.$$

下面的引理是沟通指数和与指数积分的桥梁.

引 2. 命 $f(x)$ 为在区間 (a, b) 中有微商的实函数, 而 $f'(x)$ 为单調函数并且适合 $|f'(x)| \leqslant \theta < 1$,则

$$\sum_{a<n\leqslant b} e^{2\pi i f(x)} = \int_a^b e^{2\pi i f(x)}dx + O(1).$$

由第二中值定理,立刻可以得到引 1. 又由 Euler 求和公式

$$\sum_{a<n\leqslant b} g(n) = \int_a^b g(x)dx + \int_a^b \left(x-[x]-\frac{1}{2}\right)g'(x)dx + $$
$$+ \left(a-[a]-\frac{1}{2}\right)g(a) - \left(b-[b]-\frac{1}{2}\right)g(b)$$

及 Fourier 展开

$$x-[x]-\frac{1}{2} = -\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin 2\pi nx}{n},$$

可以导出引 2.

现在由这两条引理来推导定理 1. 显然可以假定 $0<r<1$. 由于 $f'(x)$ 的单调性及 $|f'(b)-f'(a)|<(b-a)\cdot hr$, 所以可以将区間 (a, b) 分成 $\ll rh(b-a)$ 个子区間. 在每一子区間 (a', b') 中, $|f'(b')-f'(a')|\leqslant\frac{1}{2}$. 故存在整数 v, 使对任何 (a', b') 中的点 x, 都有 $|f'(x)-v|\leqslant\frac{3}{4}$. 由引 2 得到

$$\sum_{a'<x\leqslant b'} e^{2\pi i(f(x)-vx)}=\int_{a'}^{b'} e^{2\pi i(f(x)-vx)}dx+O(1).$$

而由引 1 立刻得出定理 1.

关于步驟 1), van der Corput 引入下面的"基本不等式"来代替 Буняковский-Schwarz 不等式: 命 $f(x)$ 为区間 $a+1\leqslant x\leqslant a+P$ 中的实函数, 則对适合 $2\leqslant\rho\leqslant P$ 的任何 ρ 整数都有

$$\left|\sum_{x=a+1}^{a+P} e^{2\pi if(x)}\right|\leqslant\frac{\sqrt{2}P}{\sqrt{\rho}}+\left\{\frac{4P^2}{\rho}\sum_{\sigma=1}^{\rho-1}\left|\frac{1}{P-\sigma}\sum_{x=a+1}^{a+P-\sigma} e^{2\pi i(f(x+\sigma)-f(x))}\right|\right\}^{\frac{1}{2}}. \tag{37}$$

由定理 1 及基本不等式得

定理 2. 命 $f(x)$ 为有連續 k 阶导数的实函数, 又命 $r\leqslant f^{(k)}(x)\leqslant hr$ (或 $r\leqslant -f^{(k)}(x)\leqslant hr$) 及 $b-a\geqslant 1$, 則

$$\sum_{a<n\leqslant b} e^{2\pi if(n)}\ll h^{2^{2-k}}(b-a)r^{\frac{1}{2^k-2}}+(b-a)^{1-2^{2-k}}r^{-\frac{1}{2^k-2}},$$

此处与記号 $\ll$ 有关的常数与 k 无关.

另一个处理 $k=2$ 的方法, 基础于下面的可以用初等几何証明的定理: 命 $P\geqslant 1$ 及

$$0<\vartheta\leqslant f(2)-f(1)\leqslant f(3)-f(2)\leqslant\cdots\leqslant f(P)-f(P-1)\leqslant 1-\vartheta,$$

則

$$\left|\sum_{n=1}^{P} e^{2\pi if(n)}\right|\leqslant\cot\frac{1}{2}\pi\vartheta\quad\left(\text{或}<\frac{1}{\vartheta}\right).$$

关于不等式的証明, 請参看 Кузьмин[71], Landau[72] 与 van der Corput[73] 的文章.

由这个不等式及归納法(即基本不等式)得到

定理 3. 命 $k\geqslant 2$, $f(x)$ 为在区間 $a+1\leqslant x\leqslant a+P$ 中有 k 阶导数的实函数. 若对区間 $a+1\leqslant x\leqslant a+P$ 中的全体 t 都有 $f^{(k)}(t)\geqslant r>0$ (或 $f^{(k)}(t)\leqslant -r<0$), 則

$$\left|\sum_{x=a+1}^{a+P} e^{2\pi if(x)}\right|\ll P\left(\left(\frac{r}{R^2}\right)^{\frac{1}{2^k-2}}+(rP^k)^{-\frac{1}{2^k-1}}+\left(\frac{rP}{R}\right)^{-\frac{1}{2^k-1}}\right), \tag{38}$$

此处 $R = \frac{1}{P}(f^{(k-1)}(a+p) - f^{(k-1)}(a+1))$.

定理 3 略佳于定理 1,但在許多应用中,定理 1 与定理 3 是等效的.

Van der Corput[74] 还将定理 1 进一步推广为

定理 4. 命 $f(x)$ 为在区間 $a \leqslant x \leqslant b$ 中有三阶連續导数的实函数, 而 $f'(x)$ 为递減函数,且

$$f'(a) = \alpha, \quad f'(b) = \beta.$$

又命

$$f'(x_\nu) = \nu \quad (\alpha < \nu \leqslant \beta)$$

及

$$2\pi r \leqslant |f''(x)| < Ar, \quad |f'''(x)| < AR,$$

则

$$\sum_{a<n\leqslant b} e^{2\pi i f(n)} = e^{-\frac{\pi i}{4}} \sum_{\alpha<\nu\leqslant\beta} \frac{e^{2\pi i (f(x_\nu) - \nu x_\nu)}}{|f''(x_\nu)|^{\frac{1}{2}}} + O(r^{-\frac{1}{2}}) +$$
$$+ O(\log(2+(b-a)r)) + O((b-a)r^{\frac{1}{5}}R^{\frac{1}{5}}).$$

請参看 Виноградов[75], Titchmarsh[76] 及 Phillips[77] 的文章. Titchmarsh[78] 将这方法推广到两个变数的情形,这一推广的关鍵在于估計下面形状的二重指数积分

$$\int_a^b \int_\alpha^\beta e^{if(x,y)} dx\, dy.$$

例如我們有

定理 5. 命 $f(x, y)$ 为在矩形 $a \leqslant x \leqslant b$, $\alpha \leqslant y \leqslant \beta$ $(b-a=l, \beta-\alpha=l)$ 中有三阶連續偏导数的实函数. 若在矩形中有

$$r \leqslant |f_{xx}| < Ar, \quad r \leqslant |f_{yy}| < Ar, \quad |f_{xy}| < Ar$$

与

$$|f_{xx}f_{yy} - f_{xy}^2| \geqslant r^2,$$

则

$$\int_a^b \int_\alpha^\beta e^{if(x,y)} dx dy = O\left(\frac{1+|\log l|+|\log r|}{r}\right).$$

閔嗣鶴[79] 对 Titchmarsh 定理給了一些改进.

9. Виноградов 中值定理

无論以上所說的 Weyl 方法或 van der Corput 方法,其主要之点都在于連續运用 Буняковский–Schwarz 不等式; 而这个不等式用得愈多, 精密度就愈差. 1935 年, Виноградов[24) 27) 80] 創造了一个非常精深与強有力的方法, 以后他又多次改进自己的方法. 在这一节与下一节中将要談到他的略經改进的最后結果[81]. 华罗庚指出, Виноградов 方法主要依賴于下面的中值定理.

定理 1. 命 $f(x) = \alpha_k x^k + \cdots + \alpha_1 x$ 及

$$C_k = C_k(p) = \sum_{x=a+1}^{a+P} e^{2\pi i f(x)}.$$

又命 $t_1 = t_1(k) \geqslant \frac{1}{4}k(k+1) + lk$, 則

$$\int_0^1 \cdots \int_0^1 |C_k|^{2t_1} d\alpha_1 \cdots d\alpha_k \leqslant (7t_1)^{4t_1 l} P^{2t_1 - \frac{1}{2}k(k+1)+\delta} (\log P)^{2l},$$

此处 $\delta = \delta(k) = \frac{1}{2}k(k+1)\left(1 - \frac{1}{k}\right)^l$.

由于这个定理的重要性,所以我們給出較长的摘要.

引 1. 一組整数 $(g_1, \cdots, g_b)$, $1 \leqslant g_\nu \leqslant H$, 假如它适合次之条件, 則謂之"佳位"組. 这个条件是:其中至少有 k 个,記为 $g_{i_1}, \cdots, g_{i_k}$,适合

$$g_{i_{\nu+1}} - g_{i_\nu} > 1 \quad (1 \leqslant \nu \leqslant k-1). \tag{39}$$

非"佳位"組的个数最多是

$$b!\, 3^b H^{k-1}.$$

引 2. 命 $C > 1$, $Q = RH$, $R > 1$, $H > 1$ 及

$$1 \leqslant g_1 < g_2 < \cdots < g_k \leqslant H, \quad g_\nu - g_{\nu-1} > 1,$$

此处 $g_1, \cdots, g_k$ 为整数. 又对于每一 $\nu(1 \leqslant \nu \leqslant k)$,命 x_ν 在区間

$$-w + (g_\nu - 1)R < x_\nu \leqslant -w + g_\nu R \quad (0 < w \leqslant Q)$$

中变化,則使

$$x_1^h + \cdots + x_k^h$$

分別落在长度不超过 $CQ^{\left(1-\frac{1}{k}\right)^h} (1 \leqslant h \leqslant k)$ 的区間中的整数組 $x_1, \cdots, x_k$ 的組数不超过

$$(2C)^k (2kH)^{\frac{1}{2}k(k-1)} Q^{\frac{1}{2}(k-1)}.$$

中值公式可以由归納法及下面的定理推导出来.

定理 2. 命 b 表一 $\geqslant \frac{1}{4}k(k+1) + k$ 的整数. 又命 η 为不超过

$$\frac{1}{k}\log Q / \log 2$$

的最大整数,則

$$\int_0^1 \cdots \int_0^1 |C_k(Q)|^{2b} d\alpha_1 \cdots d\alpha_k \leqslant$$

$$\leqslant (7b)^{4b} \max(1, \eta^2) Q^{2k - \frac{1}{2}(k+1) + \frac{2(b-k)}{k}} \int_0^1 \cdots \int_0^1 \left| C_k\left(Q^{1-\frac{1}{k}}\right)\right|^{2(b-k)} d\alpha_1 \cdots d\alpha_k.$$

証明分成下面三步.

a）不失一般性，可以在 $C_k(Q)$ 中假定 $a=0$. 当 $\eta<2$ 时，定理显然成立. 因此，我們假定 $\eta\geqslant 2$. 命 s 表一适合 $1\leqslant s\leqslant \eta-1$ 的整数. 将 $C_k(Q)$ 分成 2^s 部分，每份之长度 $R_s=Q2^{-s}$:

$$C_k(Q)=\sum_{g=1}^{2^s}\sum_{(g-1)R_s<x\leqslant gR_s}e^{2\pi i f(x)}=\sum_{g=1}^{2^s}Z_{sg}.$$

命 $Z=(C_k(Q))^b$，則

$$Z=\sum^{2^{sb}}Z_{sg_1}\cdots Z_{sg_b},$$

此处 $\sum^{M}$ 表一和，其項数最多是 M（在今后的証明中，常有此种了解）. 又簡书

$$Z_s=Z_{s;g_1,\cdots,g_b}=Z_{sg_1}\cdots Z_{sg_b}.$$

如果 $g_1,\cdots,g_b$ 成一"佳位"組，則 $Z_{s;g_1,\cdots,g_b}$ 称为"佳位"和，而以 Z_s' 表之. 由引 1 可知，非"佳位"和的个数不超过 $b!\,3^b2^{s(k-1)}$. 把非"佳位"和 Z_s 中的每一因子分为二份. 如此从一个非"佳位"和 Z_s 得出 2^b 个和 Z_{s+1}. 故由全体非"佳位" Z_s 中所得的"佳位"的 Z_{s+1} 的个数显然不超过

$$M_s=b!\,3^b2^{s(k-1)}\cdot 2^b=b!\,6^b2^{s(k-1)}.$$

"佳位"的 Z_{s+1} 用 Z_{s+1}' 表之. 再如前法，分割非"佳位"和. 由于 Z_1 一定是非"佳位"的，所以我們能够如此进行. 重复此項手續，由 $s=1,2,\cdots,\eta-1$，而用 Z_η' 表示由非"佳位"的 $Z_{\eta-1}$ 获得的全体 Z_η. 于是得到

$$Z=\sum_{s=1}^{\eta}\sum^{M_s}Z_s'.$$

b）由 Буняковский-Schwarz 不等式得出

$$|C_k(Q)|^{2b}=|Z|^2\leqslant\eta\sum_{s=1}^{\eta}\left|\sum^{M_s}Z_s'\right|^2\leqslant\eta\sum_{s=1}^{\eta}M_s\sum^{M_s}|Z_s'|^2. \tag{40}$$

不失一般性，可以假定 $Z_{s;g_1,\cdots,g_b}'$ $(1\leqslant s\leqslant\eta-1)$ 中的 $g_1,\cdots,g_k$ 适合(39). 把 Z_{sg_i} $(k+1\leqslant i\leqslant b)$ 分成

$$\left[\frac{Q2^{-s}}{(Q^{1-\frac{1}{k}}-1)}\right]+1\leqslant Q^{\frac{1}{k}}\cdot 2^{1-s}$$

部分，每一份的形式是

$$C^*=\sum_{w<x<w+Q'}e^{2\pi i f(x)},$$

此处 w 与 Q' 为适合

$$0\leqslant w\leqslant g_iR_s\leqslant Q,\quad 0<Q'\leqslant Q^{1-\frac{1}{k}}$$

的整数. 故由 Hölder 不等式可知

$$|Z_{sg_i}|^{2(b-k)} \leqslant \left(\sum^{Q^{\frac{1}{k}}2^{1-s}} |C^*|\right)^{2(b-k)} \leqslant (Q^{\frac{1}{k}}2^{1-s})^{2(b-k)-1} \sum^{Q^{\frac{1}{k}}2^{1-s}} |C^*|^{2(b-k)}.$$

因为

$$|Z_{sg_{k+1}} \cdots Z_{sg_b}|^2 \leqslant \frac{1}{b-k} \sum_{i=k+1}^{b} |Z_{sg_i}|^{2(b-k)},$$

故由(40)得到

$$|Z|^2 \leqslant \frac{\eta}{b-k} \sum_{s=1}^{\eta} M_s (Q^{\frac{1}{k}}2^{1-s})^{2(b-k)-1} \sum^{N_s} |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)},$$

此处 $N_s = b!\, 6^b 2^{s(k-1)}(b-k)Q^{\frac{1}{k}}2^{1-s}$. 因此

$$\int_0^1 \cdots \int_0^1 |Z|^2 d\alpha_1 \cdots d\alpha_k \leqslant \frac{\eta}{b-k} \sum_{s=1}^{\eta} M_s (Q^{\frac{1}{k}}2^{1-s})^{2(b-k)-1} \times$$

$$\times \sum^{N_s} \int_0^1 \cdots \int_0^1 |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)} d\alpha_1 \cdots d\alpha_k. \tag{41}$$

c) 积分

$$\int_0^1 \cdots \int_0^1 |Z_{sg_1} \cdots Z_{sg_k}|^2 |C^*|^{2(b-k)} d\alpha_1 \cdots d\alpha_k$$

等于下列不定方程組的解答数:

$$x_1^h + \cdots + x_k^h + y_1^h + \cdots + y_{b-k}^h = x_1'^h + \cdots + x_k'^h + y_1'^h + \cdots + y_{b-k}'^h$$
$$(1 \leqslant h \leqslant k),$$

此处变数 y 与 y' 落在形如

$$w < y, y' \leqslant w + Q' \quad (0 < Q' \leqslant Q^{1-\frac{1}{k}};\ 0 \leqslant w \leqslant Q)$$

的区間中,而 x 与 x' 則在区間

$$(g_i - 1)R_s < x_i, \quad x_i' \leqslant g_i R_s$$

之中, $s \leqslant \eta - 1$, 整数 $g_1, \cdots, g_k$ 适合条件(39).

以 $X + w$ 及 $Y + w$ 分别代替 x 及 y,則(41)式也就是方程組

$$X_1^h + \cdots + X_k^h + Y_1^h + \cdots + Y_{b-k}^h = X_1'^h + \cdots + X_k'^h + Y_1'^h + \cdots + Y_{b-k}'^h$$
$$(1 \leqslant h \leqslant k)$$

的解数,此处 Y' 在区間 $(0, Q')$ 之中,而 X_i 及 X_i' 則在

$$-w + (g_i - 1)R_s < X_i,\ X_i' \leqslant -w + g_i R_s \quad (0 \leqslant w \leqslant Q)$$

之中.

若先固定 X', 則 X 适合引 2 的要求, 其中 $R = R_s$, $C = 2(b-k)$ 及 $H = 2^s$.

所以X及X'的組数不超过

$$R_s^k\{4(b-k)\}^k(2k2^s)^{\frac{1}{2}k(k-1)}Q^{\frac{1}{2}(k-1)}=$$
$$=\{4(b-k)\}^k(2k)^{\frac{1}{2}k(k-1)}2^{\frac{1}{2}sk(k-1)-sk}Q^{2k-\frac{1}{2}(k+1)}.$$

又对已定的X及X'，Y及Y'的組数不超过

$$\int_0^1\cdots\int_0^1\left|C_k\left(Q^{1-\frac{1}{k}}\right)\right|^{2(b-k)}d\alpha_1\cdots d\alpha_k.$$

因此，当$1\leqslant s\leqslant\eta-1$时

$$\int_0^1\cdots\int_0^1|Z_{sg_1}\cdots Z_{sg_k}|^2|C^*|^{2(b-k)}\,d\alpha_1\cdots d\alpha_k\leqslant$$
$$\leqslant\{4(b-k)\}^k(2k)^{\frac{1}{2}k(k-1)}2^{\frac{1}{2}sk(k+1)-2sk}Q^{2k-\frac{1}{2}(k+1)}\times$$
$$\times\int_0^1\cdots\int_0^1\left|C_k\left(Q^{1-\frac{1}{k}}\right)\right|^{2(b-k)}d\alpha_1\cdots d\alpha_k.$$

当$s=\eta$时，由η的定义立刻得到这个不等式.

由 b)，c) 即得定理.

关于較小的k，我們还有下面的結果.

定理 3. 对于任何$\varepsilon>0$，都有

$$\int_0^1\cdots\int_0^1|C_k(P)|^\lambda d\alpha_1\cdots d\alpha_k\ll P^{\lambda-\frac{1}{2}k(k+1)+\varepsilon},$$

此处λ为k的函数，它由下面的表来定义：[32]

k	2	3	4	5	6	7	8	9	10
λ	6	16	46	110	240	414	672	1080	1770

当$k\geqslant 12$时，对于

$$\lambda\geqslant 2k^2(3\log k+\log\log k+4)-4,$$

可以得到同样的結論[23].

10. 中值定理的推論

用仍然是 Виноградов[27] 創造的“由平均至单独”的方法，我們得到下面两个重要的推論.

定理 1. 命$k\geqslant 12$，$2\leqslant r\leqslant k$及

$$\left|\alpha_r-\frac{h}{q}\right|\leqslant\frac{1}{q^2},\quad (h,q)=1,\quad 1\leqslant q\leqslant P^r.$$

又命

$$f(x)=\alpha_kx^k+\cdots+\alpha_1x.$$

则当 $P \leqslant q \leqslant P^{r-1}$ 时,

$$S = \sum_{x=1}^{P} e^{2\pi i f(x)} \ll P^{1-\frac{1}{\sigma_k}+\varepsilon},$$

此处 $\sigma_k = 2k^2(2\log k + \log\log k + 3)$[23) 83)].

定理 2. 命 k 与 P 为整数; $k \geqslant 9$, $P \geqslant 2$. 又 $f(x)$ 为在区間$(a+1, a+P)$中有$(k+1)$阶連續导数的实函数. 又設在区間$(a+1, a+P)$中有

$$1 \leqslant \lambda \leqslant \frac{f^{(k+1)}(x)}{(k+1)!} \leqslant 2\lambda$$

及

$$\lambda^{-\frac{1}{k}} \leqslant P \leqslant \lambda^{-1},$$

則

$$\sum_{x=a+1}^{a+P} e^{2\pi i f(x)} \ll e^{32k\log^2 k} P^{1-\rho}\log P,$$

此处 $\rho = (56k^2\log k)^{-1}$,而与 $\ll$ 有关的常数为絕对常数[27) 84) 85)].

这两个定理分别在 Waring 問題及素数分布問題上有着重要的应用. 現在我們将指出定理 1 証明的主要步驟. 用类似的想法可以証明定理 2.

对于 $0 < y \leqslant Y < P$, 考虑

$$S_0 = \sum_{x=1}^{P} e^{2\pi i(f(x+y)-f(x))} = \sum_{x=1}^{P} e^{2\pi i \Phi(x)},$$

此处 $\Phi(x) = Y_1 x + \cdots + Y_k x^k$; $Y_j = \binom{k}{j}\alpha_k y^{k-j} + \cdots + \binom{j+1}{j}\alpha_{j+1}y + \alpha_j$. 易知 $|S_0| - |S| \leqslant 2y$ 及

$$|S| \leqslant Y^{-1}\sum_{y=1}^{Y}|S_0| + Y.$$

由 Hölder 不等式得到

$$|S|^{2t_1} \leqslant 2^{2t_1-1}\left(Y^{-1}\sum_{y=1}^{Y}|S_0|^{2t_1} + Y^{2t_1}\right).$$

命

$$S_1 = \sum_{x=1}^{P} e^{2\pi i(\beta_1 x + \cdots + \beta_{k-1}x^{k-1} + \alpha_k x^k)}.$$

若 y 固定,则 $Y_1, \cdots, Y_{k-1}$ 亦定. 命 $\Omega(y)$ 表示适合

$$\{\beta_1 - Y_1\} \leqslant \frac{1}{2}P^{-2}Y, \cdots, \{\beta_{k-1} - Y_{k-1}\} \leqslant \frac{1}{2}P^{-k}Y, \ 0 \leqslant \beta_j \leqslant 1$$

的 $(\beta_1, \cdots, \beta_{k-1})$ 的区域. 若 $(\beta_1, \cdots, \beta_{k-1}) \in \Omega(y)$, 則

$$S_0 = S_1 + O(Y).$$

因此

$$|S|^{2t_1} \ll |S_1|^{2t_1} + Y^{2t_1}.$$

在区域 $\Omega(y)$ 上积分得

$$|S|^{2t_1} \ll P^{\frac{1}{2}k(k-1)+(k-1)}Y^{-(k-1)}\int\cdots\int_{\Omega(y)}|S_1|^{2t_1}d\beta_1\cdots d\beta_{k-1} + Y^{2t_1}.$$

現在我們給定一点 $(\beta_1, \cdots, \beta_{k-1})$，而来估計包含此点的区域 $\Omega(y)$ 的数目. 可以証明，$\Omega(y)$ 的个数不超过 $1 + \frac{Y}{q} + \frac{Yq}{P^r}$，换言之，单位立方体

$$0 \leqslant \beta_1 < 1, \ \cdots, \ 0 \leqslant \beta_{k-1} < 1$$

中的每一点最多被 $\ll \frac{Y}{q} + \frac{Yq}{P^r} + 1$ 个区域 $\Omega(y)$ 所遮盖. 因此

$$|S|^{2t_1} \ll P^{\frac{1}{2}k(k-1)+k-1}Y^{-k}\sum_{y=1}^{Y}\int\cdots\int_{\Omega(y)}|S_1|^{2t_1}d\beta_1\cdots d\beta_{k-1} + Y^{2t_1} \ll$$

$$\ll P^{\frac{1}{2}k(k-1)+k-1}Y^{-k}\left(\frac{Y}{q} + \frac{Yq}{P^r} + 1\right)\int_0^1\cdots\int_0^1|S_1|^{2t_1}d\beta_1\cdots d\beta_{k-1} + Y^{2t_1}.$$

这个不等式是很重要的，它是沟通"平均"与"单独"的桥梁. 由中值定理及一些計算即得定理 1.

11. 羣的特征

命 $\mathfrak{G}$ 为一交换羣. 若 $\chi(n)$ 为 $\mathfrak{G}$ 上定义的复函数，且对 $\mathfrak{G}$ 中的全体元素 a, b，都有 $\chi(a) \neq 0$ 及 $\chi(ab) = \chi(a)\chi(b)$，则称 $\chi(n)$ 为特征.

若对全体 $a \in \mathfrak{G}$ 都有 $\chi(a) = 1$，则称此特征为主特征. 記之为 $\chi_0(a)$.

若 $\mathfrak{G}$ 有有限阶 g，则习知 $\mathfrak{G}$ 可以表成阶分别为 $g_1, \cdots, g_s$ 的巡迴羣 $\mathfrak{G}_1, \cdots, \mathfrak{G}_s$ 的直乘积. 换言之，$\mathfrak{G}$ 的每一元素 a 可以唯一地表为 $a_1^{l_1}\cdots a_s^{l_s}$，此处 $a_i \in \mathfrak{G}_i$ 及

$$0 \leqslant l_i < g_i.$$

命 $\chi_u(a_i) = e^{2\pi i u a_i/g_i}$ 为 $\mathfrak{G}_i$ 的一个特征，则

$$\chi(a) = \chi_{u_1}(a_1^{l_1})\cdots\chi_{u_s}(a_s^{l_s}) = \prod_{\nu=1}^{s} e^{2\pi i u_\nu l_\nu/g_\nu}, \quad 0 \leqslant u_\nu < g_\nu$$

为 $\mathfrak{G}$ 的一个特征. 因此我們得到 $\mathfrak{G}$ 的 $g_1\cdots g_s = g$ 个互不相同的特征. 易証，这些就是羣 $\mathfrak{G}$ 的全体特征. 由此可得下面两个基本关系式:

$$\sum_{a\in\mathfrak{G}}\chi(a)\chi'(a) = \begin{cases}0, & 若\ \bar{\chi} \neq \chi'; \\ g, & 若\ \bar{\chi} = \chi'\end{cases} \tag{42}$$

及

$$\sum_{\chi}\chi(a)\chi(b) = \begin{cases}0, & 若\ a \neq b^{-1}; \\ g, & 若\ a = b^{-1}.\end{cases} \tag{43}$$

例 1. 命 $\mathfrak{G}$ 为全体整数所成的加法羣，則对于每一实数 α，可得一对整数 n 定义的特征

$$\chi(n) = e^{2\pi i\alpha n}.$$

例 2. 命 $\mathfrak{G}$ 为 mod q 的剩余类的加法羣，則对每一整数 a mod q，函数

$$\chi(n) = e^{2\pi i a n/q}$$

为 $\mathfrak{G}$ 的一个特征. 这称为 mod q 的加性特征. 易証，这些就是 mod q 的全体加性特征.

例 3. 命 p 为一素数，而 $\mathfrak{G}$ 为 mod p 的縮剩余系所成的乘法羣，則对每一 a，函数

$$\chi(n) = e^{2\pi i a \operatorname{ind} n/(p-1)}$$

为 $\mathfrak{G}$ 的一个特征. 同样可証，这些就是 mod p 的全体乘性特征.

例 4. 更一般些，命 $\mathfrak{G}$ 为 mod q 的縮剩余系所成的乘法羣，$q = 2^{l_{s+1}}p_1^{l_1}\cdots p_s^{l_s}$，此处 $p_1, \cdots, p_s$ 为互不相同的奇素数. 当 $i = 1, 2, \cdots, s$ 时，定义

$$\chi_i(n) = \chi_{a_i}(n) = e^{2\pi i a_i \operatorname{ind} n/\varphi(p_i^{l_i})} \quad (1 \leqslant a_i \leqslant \varphi(p_i^{l_i})).$$

又当 $l_{s+1} \geqslant 2$ 时，定义

$$\chi_{s+1}(n) = \begin{cases}(-1)^{\frac{1}{2}(n-1)a}, & a = 1, 2, \quad 若\ l_{s+1} = 2;\\ (-1)^{\frac{1}{2}(n-1)a}e^{2\pi icb/2l-2}, & a = 1, 2\ 及\ 1 \leqslant c \leqslant 2^{l-2}, \quad 若\ l_{s+1} > 2,\end{cases}$$

此处 b 为由 $n \equiv (-1)^{\frac{1}{2}(n-1)}5^b \pmod{2^l}$，及 $b \geqslant 0$ 定义的整数，則我們得到 mod q 的全体特征

$$\chi(n) = \chi_{s+1}(n)\chi_1(n)\cdots\chi_s(n), \quad (n, q) = 1.$$

为了方便起見，当 $(n, q) > 1$ 时，常常定义

$$\chi(n) = 0.$$

若 mod q 的特征 $\chi(n)$ 滿足下之条件，卽存在 q 的眞因子 q' 使对适合 $n \equiv n' \pmod{q'}$ 及 $(n, q) = (n', q) = 1$ 的全体 n 及 n' 都有 $\chi(n) = \chi(n')$，則称 $\chi(n)$ 为非原特征. 否則，称 $\chi(n)$ 为原特征.

12. 特 征 和

常称首項为 1 的多項式为正則多項式. 命 $[q]$ 为含 q 个元素的域，$f(x)$ 为 $[q]$ 上的 k 次旣約多項式，$\chi(n)$ 为 $[q]$ 的乘性特征. 常用 (f, g) 表示两个多項式 $f(x)$ 与 $g(x)$ 的結式. 又对于任意 ν 次正則多項式 $g(x)$，常置 $|g(x)| = q^\nu$. 定义

$$L(f, \chi, s) = \sum_g \frac{\chi(f, g)}{|g|^s}, \tag{44}$$

此处的和号系对 $[q]$ 上的全体正则多项式求和。显然

$$L(f, \chi, s) = \sum_{\nu=0}^{\infty} \frac{\sigma_\nu}{q^{\nu s}}, \tag{45}$$

此处 $\sigma_\nu = \sum_g \chi(f, g)$，而其中的 g 通过全体 ν 次多项式。因 $\chi(f, g)$ 与 $|g|$ 都是 g 的积性函数，故得

$$L(f, \chi, s) = \prod_G \left(1 - \frac{\chi(f, G)}{|G|^s}\right)^{-1}, \tag{46}$$

此处的乘号系对 $[q]$ 上的全体正则既約多项式求积。以下常假定 $\chi^k \neq \chi_0$.

定理 1. $L(f, \chi, s)$ 为 q^{-s} 的 $k-1$ 次多项式.

只要証明当 $\nu \geqslant k$ 时，$\sigma_\nu = 0$ 即可。命 ϑ 为 $f(x) = 0$ 的一根，并記，由$[q]$添加 ϑ 所成的域为 $[q^k]$，则

$$(f, g) = (-1)^{k\nu}(g, f) = (-1)^{k\nu}Ng(\vartheta),$$

此处 $N(\alpha)$ 表示 $[q^k]$ 中的元素关于 $[q]$ 的矩。命 ψ 为 $[q^k]$ 上的延拓特征，即

$$\psi(g(\vartheta)) = \chi(-1)^{k\nu}\chi(f, g),$$

此处 ν 为 g 的次数。記 $g(x) = x^\nu + a_{\nu-1}x^{\nu-1} + \cdots + a_0$，则得

$$\sigma_\nu = \sum_{a_0 \in [q]} \cdots \sum_{a_{\nu-1} \in [q]} \chi(f, g) = \varepsilon^\nu \sum_{a_0 \in [q]} \cdots \sum_{a_{\nu-1} \in [q]} \psi(g(\vartheta)),$$

此处 $\varepsilon = \chi^k(-1)$。当 $\nu \geqslant k$ 时，固定 $a_k, \cdots, a_{\nu-1}$，当 $a_0, \cdots, a_{k-1}$ 各自通过 $[q]$ 的全体元素时，$g(\vartheta)$ 通过域 $[q^k]$ 的全体元素。因此当 $\nu \geqslant k$ 时，

$$\sigma_\nu = \varepsilon^\nu q^{\nu-k} \sum_{\xi \in [q^k]} \psi(\xi) = 0.$$

定理 2. 命

$$S(f, \chi) = \sum_{x \in [q]} \chi(f(x)),$$

则

$$S(f, \chi) = q^{s_1} + \cdots + q^{s_{k-1}}, \tag{47}$$

此处 $s_1, \cdots, s_{k-1}$ 表示 $L(f, \chi, s)$ 的零点.

在(46)式两端取对数，便得

$$\log L(f, \chi, s) = \sum_G \sum_{\nu=1}^{\infty} \frac{1}{\nu} \chi(f, G^\nu) |G^\nu|^{-s}.$$

另一方面，

$$\log L(f, \chi, s) = -\sum_{h=1}^{\infty} \frac{1}{h} \left(\sum_{i=1}^{h-1} q^{hs_i}\right) q^{-hs}.$$

比較 q^{-s} 的系数，得到

$$-\sum_{i=1}^{k-1} q^{s_i} = \sum_{|G^\nu|=q} \frac{1}{\nu} \chi(f, G^\nu) = \sum_{a\in[q]} \chi(f, x-a) = \sum_{a\in[q]} \chi(f(a)). \quad (48)$$

由(48)可知，欲估計特征和 $\sum_{a\in[q]} \chi(f(a))$，只要估計 $q^{s_1}+\cdots+q^{s_{k-1}}$ 便已足够。假如我們能够証明 $L(f, \chi, s)$ 的零点的实部都是 $\sigma=\frac{1}{2}$，則得

$$\left|\sum_{a\in[q]} \chi(f(a))\right| \leqslant (k-1)\sqrt{q}.$$

关于这个問題，A. Weil 作出了重要的貢献。命 Ω 为 $[q]$ 上的代数函数域，定义 ζ-函数

$$\zeta_\Omega(s) = \sum_{\mathfrak{A}} \frac{1}{|N(\mathfrak{A})|^s} = \prod_{\sigma} \left(1 - \frac{1}{|N(\sigma)|^s}\right)^{-1},$$

此处 $\mathfrak{A}$ 經过 Ω 的全体整因子，而 σ 則經过 Ω 的全体素因子，又 $|N(\mathfrak{A})|$ 表示絕对矩。$\zeta_\Omega(s)$ 是一个具有周期 $2\pi i/\log q$ 的周期函数，它在整个平面上，除了在 $s\equiv 0, 1 \pmod{2\pi i/\log q}$ 处有一次极之外，都是正則的。

定理 3 (A. Weil). $\zeta_\Omega(s)$ 的零点的实部都等于 $\frac{1}{2}$.

这个定理原来是 Artin 提出来的一个重要猜想。对椭圓函数域的特殊情形，Hasse[85] 給予了証明。而一般情形則由 A. Weil[87] 在 1948 年完全解决(参看 Igusa[88] 与 Roquette[89] 的文章)，因为在 Weil 的証明中，需要用到代数几何[90]的全部知識，所以很难在此作一簡单的概述。

Weil[91] 給出了定理 3 的另一推論。

定理 4. 关于 Kloostermann 和，我們有下面的估計：

$$\left|\sum_{x=1}^{p-1} e^{2\pi i\left(cx+\frac{d}{x}\right)/p}\right| \leqslant 2\sqrt{p}. \quad (49)$$

Carlitz 与 Uchiyama[92] 还由定理 3 推出了下面的結果：

定理 5. 命 $f(x)=a_kx^k+\cdots+a_1x+a_0$, $p\nmid a_k$, 則

$$\left|\sum_{x=1}^{p-1} e^{2\pi i f(x)/p}\right| \leqslant k\sqrt{p}. \quad (50)$$

关于 Kloostermann[93] 和的估計的历史如下：在研究将整数表成 $ax^2+by^2+cz^2++dw^2$ 的形式的时候，Kloostermann 首先引入了这种类型的和，所以通常就称之为 Kloostermann 和。他得到的估計为 $O(p^{\frac{3}{4}})$。以后 Salié[94] 与 Davenport[95] 又将此估計改进为 $O(p^{\frac{2}{3}+\varepsilon})$.

关于 (50) 的估計的历史如下：Mordell[96] 証明它的阶为 $O(p^{1-\frac{1}{k}})$，以后 Davenport[95] 又得到了估計 $O(p^{1-\frac{1}{m}})$，此处 m 为形状如 2^g 与 $3\cdot 2^g$，而又不超过 k 的整数中的最大者．因为 Mordell 方法很有启发性，所以我們在这里概要地叙述其証明过程：表达式

$$\frac{1}{p^k}\sum_{a_k=1}^{p}\cdots\sum_{a_1=1}^{p}\left|\sum_{x=1}^{p}e^{2\pi i(a_kx^k+\cdots+a_1x)/p}\right|^{2k}$$

等于同余式組

$$\sum_{i=1}^{k}x_i^h\equiv\sum_{i=1}^{k}y_i^h\ (\bmod p),\quad 1\leqslant h\leqslant k,\quad 1\leqslant x,\ y\leqslant p$$

的解数．显然解数 $\leqslant k!\,p^k$．进而言之，他証明了，对于固定的 $f(x)=a_kx^k+\cdots+a_1x$，$p\nmid a_k$，存在 $\gg p^2$ 个不同的多項式 $f(\lambda x+\mu)\bmod p$，使 $\left|\sum_{x=1}^{p}e^{2\pi if(\lambda x+\mu)/p}\right|$ 等于 $\left|\sum_{x=1}^{p}e^{2\pi if(x)/p}\right|$．因此

$$\left|\sum_{x=1}^{p}e^{2\pi if(x)/p}\right|^{2k}\ll p^{2k(1-\frac{1}{k})}.$$

故得定理．

华罗庚与閔嗣鶴[97] 将这一結果推广到两个变数的情形，即

$$\sum_{x=1}^{p}\sum_{y=1}^{p}e^{2\pi if(x,y)/p}\ll p^{2-\frac{2}{k}},$$

此处 $f(x,y)$ 为一 k 次多項式．我們假定它不能化成一个变数的多項式，用 Weil 方法，希望可能得到某些改进．

13. 完整三角和

命 q 表一 $\geqslant 1$ 的整数，$f(x)$ 为一整系数的 k 次多項式，并且 $f(0)=0$，即

$$f(x)=a_kx^k+\cdots+a_1x.$$

我們現在研究指数和

$$S(q,f(x))=\sum_{x=1}^{q}e^{2\pi if(x)/q}.\tag{51}$$

华罗庚[98] 在 1940 年証明了下面的結果：

定理 1. 若 $(a_k,\cdots,a_1,q)=1$，则

$$S(q,f(x))\ll q^{1-\frac{1}{k}+\varepsilon},$$

此处 ε 为一任給的正数，而与 $\ll$ 有关的常数仅依賴于 k 及 ε.

証. 当 $(q_1, q_2) = 1$ 时,

$$S(q_1q_2, f(x)) = S(q_1, f(q_2x)/q_2)\, S(q_2, f(q_1x)/q_1).$$

因此, 欲計算(或估計)(51), 只要計算当 $q = p^l$ 时的情况便已足够,此处 p 为素数. 当 $l = 1$ 时,此即 § 12 中証明的定理. 現在对 l 用归納法.

由 $p^t \| (ka_k, \cdots, a_1)$ 来定义 t. 当 $l < 2(t+1)$ 时, 定理显然成立. 当 $l \geqslant$ $\geqslant 2(t+1)$ 时,置

$$S(p^l, f(x)) = \sum_{\nu=1}^{p} \sum_{\substack{0 \leqslant x < p^l \\ x \equiv \nu \pmod p}} e^{2\pi i f(x)/p^l} = \sum_{\nu=1}^{p} S_\nu.$$

若 ν 非同余式 $f'(x) \equiv 0 \pmod{p^{t+1}} (0 \leqslant x < p)$ 的解,則得 $S_\nu = 0$. 若 ν 为同余式 $f'(x) \equiv 0 \pmod{p^{t+1}}$ $(0 \leqslant x < p)$ 的解, 則易見能整除 $f(\nu + py) - f(\nu)$ 全体系数的 p 的最高方冪 p^{σ_ν} 适合 $p \leqslant p^{\sigma_\nu} \leqslant p^k$. 因此

$$|S_\nu| = \left|\sum_{y=0}^{p^{l-1}} e^{2\pi i f(\nu+py)/p^l}\right| \leqslant p^{\sigma_\nu\left(1-\frac{1}{k}\right)} |S(p^{l-\sigma_\nu}, g_\nu(x))|,$$

此处 $g_\nu(x) = p^{-\sigma_\nu}(f(\nu + px) - f(\nu))$. 若能整除 $g'_\nu(x)$ 全体系数的 p 的最高方冪为 p^u,則易証同余式 $g'_\nu(x) \equiv 0 \pmod{p^{u+1}}$的解数不超过同余式 $f'(x) \equiv 0 \pmod{p^{t+1}}$ $(0 \leqslant x < p)$ 的根 ν 的重数. 故由归納法即得定理.

同法,我們可以証明,若 $p^{-t}f'(x) \equiv 0 \pmod p$ 的根的重数 $\leqslant m$,則

$$S(f(x), p^l) = O\left(p^{l\left(1-\frac{1}{m+1}\right)}\right).$$

华罗庚[99] 还将他的定理推广到有理数域上的任何 n 次代数数域上去.

14. 不完整和的估計方法

命 $g(x)$ 为有周期 q 的函数,对于 $0 \leqslant x < q$ 显然有

$$g(x) = \frac{m}{q} + \frac{1}{q}\sum_{n=1}^{q-1} e^{2\pi i n\frac{x}{q}}\left(1 - e^{-2\pi i m\frac{n}{q}}\right)\Big/\left(1 - e^{-2\pi i\frac{n}{q}}\right) =$$

$$= \begin{cases} 1, & 若\ 0 \leqslant x < m; \\ 0, & 若\ m \leqslant x < q. \end{cases}$$

因此

$$\sum_{x=0}^{m-1} f(x) = \sum_{x=0}^{q-1} f(x) g(x) =$$

$$= \frac{m}{q}\sum_{x=0}^{q-1} f(x) + \frac{1}{q}\sum_{x=0}^{q-1} f(x) \sum_{n=1}^{q-1} e^{2\pi i n\frac{x}{q}}\left(1 - e^{-2\pi i m\frac{n}{q}}\right)\Big/\left(1 - e^{-2\pi i\frac{n}{q}}\right).$$

故得

$$\left|\sum_{x=0}^{m-1} f(x) - \frac{m}{q}\sum_{x=0}^{q-1} f(x)\right| \leqslant \sum_{n=1}^{q}\frac{1}{n}\left|\sum_{x=0}^{q-1} f(x) e^{2\pi i\frac{nx}{q}}\right|. \tag{52}$$

由此可以将不完整和的估計归結为完整和的估計．例如[100]，当 $1 \leqslant m \leqslant q$ 时，

$$\sum_{x=1}^{m} e^{2\pi i\frac{f(x)}{q}} \ll q^{1-\frac{1}{k}+\varepsilon} d^{\frac{1}{k}}, \tag{53}$$

此处 $(a_k, \cdots, a_2, q) = d$，而与 $\ll$ 有关的常数仅依賴于 ε 及 k.

类似地，若

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{qP^{k-1}},$$

則由部分求和得到

$$\sum_{x=1}^{P} e^{2\pi i f(x)\alpha} \ll Pq^{-\frac{1}{k}+\varepsilon}. \tag{54}$$

命 $p > 2$ 为素数，$(a, p) = 1$．若 $x^n \equiv a \pmod p$ 有解，則称 a 为 mod p 的 n 次剩余，否則称 a 为非剩余.

命 χ 为 mod p 之原特征．特征和 $S(m) = \sum_{n \leqslant m} \chi(n)$ 的估計在解析数論中有着重要意义．例如 Линник 与 Rényi[101] 証明了：命 $N^*_{\min}$ 表示使 $\chi(n) \neq 1$ 成立的絕对值最小 $(\neq 0)$ 的整数 n，則或者当 $p > p_0(\varepsilon)$ 时，$N^*_{\min} < p^{\varepsilon}$，或者 $|S(m)| \ll \sqrt{p}$.

下面是习知的 Pólya[102] 的結果：对于所有的特征 $\chi \neq \chi_0 \bmod p$，都有

$$|S(m)| < \sqrt{p}\log p.$$

由此立刻可知，最小正二次非剩余 $N_{\min} < \sqrt{p}\log p$.

关于 $N_{\min}$ 的上界的估計，至今最好的結果还是属于 Виноградов[103] 的．他得到如下的結果：

定理． 若 n 为 $p-1$ 的异于 1 的因子，則对于全体充分大的 p，mod p 的最小 n 次非剩余

$$\leqslant p^{\frac{1}{2k}}(\log p)^2, \quad k = e^{\frac{n-1}{n}}.$$

特別由此得出 $N_{\min} \leqslant T = p^{\frac{1}{2\sqrt{e}}}(\log p)^2$.

这个結果的証明是很簡易的．事实上，若区間 $[1, T]$ 中的全体整数都是二次剩余，則不超过 $Q = \sqrt{p}\log^2 p$ 的二次非剩余都有一素因子 q 适合 $T < q \leqslant Q$．因此，不超过 Q 的二次非剩余的个数 N 适合

$$N \leqslant \sum_{T<q\leqslant Q}\left[\frac{Q}{q}\right] < Q\sum_{T<q\leqslant Q}\frac{1}{q}.$$

不难証明

$$\sum_{T<p\leqslant Q}\frac{1}{p}=\log\frac{\log Q}{\log T}+O\left(\frac{1}{\log Q}\right).$$

因此，由上面的不等式及习知的結果

$$N=\frac{1}{2}Q+\frac{\theta}{2}\sqrt{p}\log p,\quad |\theta|\leqslant 1$$

卽得定理.

在广义 Riemann 猜想之下，Ankeny[104] 証明了：

$$N_{\min}\ll(\log p)^2.$$

由 Pólya 定理及下面习知的等式：

$$\sum_{k\mid p-1}\frac{\mu(k)}{\varphi(k)}\sum_{\chi^{(k)}}\sum_{n=1}^{g(p)-1}\chi^{(k)}(n)=0, \tag{55}$$

此处 $g(p)$ 表示 p 的最小正原根，而 $\chi^{(k)}$ 通过 mod k 的全体 $\varphi(k)$ 个特征. Виноградов[105] 証明了

$$g(p)=O(2^m\sqrt{p}\log\log p),$$

此处 m 表示 $p-1$ 的不同的素因子个数.

华罗庚用

$$\sum_{k\mid p-1}\frac{\mu(k)}{\varphi(k)}\sum_{\chi^{(k)}}\sum_{a=0}^{|h(p)|-1}\sum_{n=-a}^{a}\chi^{(k)}(n)=0$$

代替(55)，此处 $h(p)$ 表示 p 的有最小絕对值的原根；同时証明：对于全体非主特征 $\chi(n)$，都有

$$\frac{1}{A+1}\left|\sum_{a=0}^{A}\sum_{n=-a}^{a}\chi(n)\right|\leqslant\sqrt{p}-\frac{A+1}{\sqrt{p}},\quad 1\leqslant A<p. \tag{56}$$

由此他[106]得到了

$$|h(p)|<2^m\sqrt{p}$$

及

$$g(p)<2^{m+1}\sqrt{p}.$$

Erdös[107] 用 Brun 方法証明了：对于充分大的 p，有

$$g(p)<p^{\frac{1}{2}}\log^{17}p.$$

在广义 Riemann 猜想下，Ankeny[104] 証明了：

$$g(p)=O(2^m\log^2 p\log^2(2^m\log p)).$$

关于 $g(p)$ 的下界的估計，Turan[108] 証明了：

$$g(p)=\Omega(\log p).$$

华罗庚[109]还用(56)証明了:

$$\log \varepsilon < \sqrt{d}\left(\frac{1}{2}\log d + 1\right),$$

此处 $\varepsilon = (x_0 + \sqrt{d}\, y_0)/2$; x_0, y_0 为 Pell 方程 $x^2 - dy^2 = 4$ 的最小正解,而 d 为 $\equiv 0$ 或 1 (mod 4) 的非平方正整数.

这个結果是下面 Schur[110] 定理的改进:

$$\log \varepsilon < \sqrt{d}\left(\frac{1}{2}\log d + \frac{1}{2}\log\log d + 1\right).$$

在所有上面說到的关于 $N_{\min}$, $g(p)$ 与 $\log \varepsilon$ 的定理的証明中,都曾用到

$$\tau(\chi) = \sum_{n=1}^{p} \chi(n) e^{2\pi i \frac{n}{p}}.$$

不难証明,对于 mod p 的原特征,有

$$|\tau(\chi)| = \sqrt{p}.$$

而对于 mod p 的实原特征,則有确切的数值:

$$\tau(\chi) = \begin{cases} \sqrt{p}, & 若\ \chi(-1) = 1; \\ i\sqrt{p}, & 若\ \chi(-1) = -1. \end{cases}$$

关于素数为变数的特征和, Линник[111] 得到下面的定理:

定理 1. a) 对于 mod q 的复特征 $\chi(n)$,有

$$\sum_{p \leqslant N} \chi(p) \ll \frac{N}{\log N}\left\{\exp\left(-c_0 \frac{\log N}{\log q}\right) + \frac{1}{\log q}\right\}.$$

b) 命 $-q < 0$ 为基本判別式,則

$$\sum_{p<N} \left(\frac{-q}{p}\right) \ll \frac{N}{\log N}\left\{\exp\left(-c_0 \frac{\log N}{\log q}\right) + \exp\left(-c_0 \frac{h(-q)}{\sqrt{q}} \log N\right) + \frac{1}{\log q}\right\},$$

此处 $h(-q)$ 为 $k(\sqrt{-q})$ 的类数,而 c_0 为一絕对常数.

Линник 这个結果的証明主要依賴于下面的引理.

引. 命 $\chi(n)$ 为 mod q 的一个实的或复的特征, $L(s, \chi)$ 为与它对应的 L-函数,則存在絕对常数 c,使当 $q \to \infty$ 时, $L(s, \chi)$ 在临界区域中的零点 $\rho_k = \beta_k + it_k$ 适合

$$\sum_{\rho_k} \frac{m_k}{|\rho_k|^2} \exp(-c\sigma_k \log q) \ll 1,$$

此处 m_k 为零点 ρ_k 的重数,而 $\sigma_k = 1 - \rho_k$.

Paley[112] 証明了: 存在正常数 A, 两个正整数貫 (n_ν) 与 (q_ν) 及原特征貫 χ_ν mod q_ν,

使

$$\left|\sum_{m=1}^{n_\nu} \chi_\nu(m)\right| \geqslant A\sqrt{q_\nu}\log\log q_\nu \quad (\nu = 1, 2, \cdots).$$

以后，Chowla[113] 又在同样的假定下証明了

$$\sum_{m=1}^{n_\nu} \chi_\nu(m) \geqslant A\sqrt{q_\nu}\log\log q_\nu.$$

Batman, Chowla 与 Erdös[114] 在 1950 年得到了同样类型的結果,但其中 q 限制为素数. 这一結果,以往 Chowla[115] 曾在广义 Riemann 猜想下得到过. 因为在百科全书中,还有关于特殊 Dirichlet 級数及其应用的专著,所以这类結果就不在此詳細闡述了.

15. 素数变数的指数和

我們現在来介紹 Виноградов[10) 27)]关于估計素数变数的指数和的开創性方法. 他是首先給出这种和以非无聊估計的人. 依靠这个估計，他証明了著名的“三素数定理”. 这种和的形状为

$$\sum_{p\leqslant N} e^{2\pi i f(p)},$$

此处 p 通过不超过 N 的全体素数. 首先,我們要指出在 Виноградов 工作中經常用到的一个重要原則;他常常将他研究的問題归結为下面形状的二重指数和的估計:

$$\sum e^{2\pi i\alpha uv},$$

此处 u 与 v 分别通过某个整数集合. 在用这个方法时，u 与 v 常常是大量其他变量的函数. 一般言之,当 u 与 v 的分布有一定程度的規則时,我們就可能对上面的和进行估計. 将这个原則应用到所研究的問題时,依賴于下面的引理.

引. 假定我們有三个由正整数組成的递增貫；u 取全体 u_1u_2，此处 u_1 經过第一貫中的全体整数，u_2 独立地經过第二貫中的全体整数，而 v 則經过第三个整数貫,又假定

$$1 < U < N,\quad U < U' \ll U,\quad \alpha = \frac{h}{q} + \frac{\theta}{q^2},\quad (h, q) = 1,\quad 1 < q < N$$

及

$$S = \sum_{U<u\leqslant U'} \sum_{v\leqslant\frac{N}{u}} e^{2\pi i\alpha uv},$$

則

$$S \ll L^2N(q^{-1} + qN^{-1} + U^{-1} + UN^{-1})^{\frac{1}{2}},$$

此处 $L = \log N$.

證. 命 $\xi(z)$ 为 $z = u_1u_2$ 的解数,则

$$S = \sum_{U<z\leqslant U'} \xi(z) \sum_{v\leqslant\frac{N}{z}} e^{2\pi i azv},$$

此处 z 經过所示区間中的全体整数. 于是由 Буняковский–Schwarz 不等式得到

$$S^2 \ll \sum_{U<z\leqslant U'} \xi^2(z) \sum_{U<z\leqslant U'} \left|\sum_{v\leqslant\frac{N}{z}} e^{2\pi i azv}\right|^2 \ll UL^3 \sum_{U<z\leqslant U'} \sum_{v\leqslant\frac{N}{z}} \sum_{v'\leqslant\frac{N}{z}} e^{2\pi i az(v-v')} =$$

$$= UL^3 \sum_{v\leqslant\frac{N}{z}} \sum_{v'\leqslant\frac{N}{z}} \sum_{U<z<\min\left(\frac{N}{v}, \frac{N}{v'}, U'\right)} e^{2\pi i az(v-v')} \ll UL^3 \sum_{v\leqslant\frac{N}{z}} \sum_{v'\leqslant\frac{N}{z}} \min\left(U, \frac{1}{\{\alpha(v-v')\}}\right).$$

对于每一固定的 v, 将里面的和分为 $\ll \frac{N}{Uq} + 1$ 个长度都 $\leqslant q$ 的分和. 由于每一分和都 $\ll U + q\log q$ 及 $\log q < \log N = L$,所以

$$S^2 \ll UL^3(NU^{-1})(NU^{-1}q^{-1} + 1)(U + q\log q) \ll$$

$$\ll N^2L^4(q^{-1} + qN^{-1} + U^{-1} + UN^{-1}).$$

我們概述下面的定理来作为 Виноградов 方法的典型例子.

定理 1. 命 $N \geqslant 1$, $L = \log N$ 及 $H = e^{\frac{1}{2}\sqrt{L}}$,又命

$$\left|\alpha - \frac{h}{q}\right| < \frac{1}{q^2}, \quad (h, q) = 1, \quad 1 < q < N,$$

则

$$S(\alpha) = \sum_{p\leqslant N} e^{2\pi i\alpha p} \ll NL^5\left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right).$$

定理的証明可以划分为下面三个步驟.

1)(篩法). 命 $P = \prod_{p\leqslant\sqrt{N}} p$ 为全体 $\leqslant \sqrt{N}$ 的素数的乘积, 则

$$S(\alpha) = \sum_{n\leqslant N}\left(\sum_{d|(P, n)} \mu(d)\right)e^{2\pi i\alpha n} + O(\sqrt{N}) =$$

$$= \sum_{d|P} \mu(d) \sum_{0\leqslant m\leqslant\frac{U}{d}} e^{2\pi i\alpha dm} + O(\sqrt{N}). \tag{57}$$

将区間 $0 < m \leqslant N$ 分为形如

$$M \leqslant m \leqslant M'$$

的子区間,此处 $M < M' \leqslant 2M$,这种区間的个数为 $O(L)$. 于是定理归結为去証明

$$S(M) = \sum_{d|P} \mu(d) \sum_{\substack{M<m\leqslant M'\\ m\leqslant\frac{N}{d}}} e^{2\pi i\alpha dm} \ll NL^4\left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right).$$

2)(消去比較容易的部分). 当 $M \geqslant H$ 时,

$$S(M) \ll NL\left(\frac{q}{N} + \frac{1}{q} + \frac{1}{H}\right)$$

当 $M < H$ 时，$S(M)$ 中的与只含有 $\leqslant H^2$ 的素因子的 d 相应的各项之和显然 $\ll NH^{-1}$.

現在我們来研究和

$$\sum_{M<m\leqslant M'} \sum_{d\leqslant \frac{N}{m}} \mu(d) e^{2\pi i a d m},$$

此处 $M < H$,而 d 經过 P 的全体那种因子，卽至少含有一个 $> H^2$ 的素因子者．将上面的和記为

$$\sum_k S_k'(M) - \sum_k S_k''(M),$$

此处

$$S_k'(M) = \sum_{M<m\leqslant M'} \sum_{d\leqslant \frac{N}{m}} e^{2\pi i a d m},$$

而 d 經过 P 的满足下面条件的全体因子: $\mu(d) = 1$,而且 d 正好有 k 个素因子 $>H^2$. $S_k''(M)$ 的定义是类似的,仅需在 $S_k'(M)$ 的定义中将 $\mu(d) = 1$ 换为 $\mu(d) = -1$.

因为 $\leqslant N$ 的数最多只有 $\ll L$ 个素因子,所以 k 的最大値亦 $\ll L$. 因此，問題归結为去証明

$$S_k'(M) \ll NL^3\left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right);$$

又对 $S_k''(M)$ 也有同样的估計.

3) 命

$$T_k(M) = \sum_{M<m\leqslant M'} \sum_{pt\leqslant \frac{M}{m}} e^{2\pi i a p t m},$$

此处 p 通过适合 $H^2 < p \leqslant \sqrt{N}$ 的全体素数，而 t 通过 P 的具有下面条件的全体因子; t 正好有 $k-1$ 个 $> H^2$ 的素因子而且 $\mu(t) = -1$. 于是

$$|S_k'(M)| \leqslant \frac{1}{k}|T_k(M)| + O(NH^{-2}) \leqslant |T_k(M)| + O(NH^{-2}).$$

为了估計 T_k，我們将区間 $H^2 < p \leqslant \sqrt{N}$ 分成 $\ll L$ 个形为 $Q < p \leqslant Q'$ 的子区間,此处 $Q < Q' \ll Q$. 因此,只要証明

$$T_k(M, Q) = \sum_{M<m\leqslant M'} \sum_{Q<p\leqslant Q'} \sum_{mpt\leqslant N} e^{2\pi i a p t m} \ll NL^2\left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right)$$

便已足够.

現在来应用引理．取 $u = mp$, $v = t$,其中 t 满足上面所說的条件．因为引理之 U 在此为 MQ,故得

$$T_k(M, Q) \ll NL^2(q^{-1} + qN^{-1} + M^{-1}Q^{-1} + MQN^{-1})^{\frac{1}{2}} \ll$$
$$\ll NL^2((q^{-1} + qN^{-1})^{\frac{1}{2}} + H^{-1}).$$

定理証完.

Виноградов[116] 将他自己的定理推广为更一般的結果. 例如,我們得到下面的定理.

定理 2. 命 $0 < Q \leqslant C_1(k)L^{\sigma_1}$,

$$f(x) = \frac{h}{q}x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k, \quad (h, q) = 1,$$

此处 $\alpha_i (1 \leqslant i \leqslant k)$ 都是实数, 而 $L^\sigma < q \leqslant P^k L^{-\sigma}$. 則对任何 $\sigma_0 > 0$, 当 $\sigma > 2^{6k} \cdot$ $\cdot (\sigma_0 + \sigma_1 + 1)$ 时,

$$\left| \sum_{\substack{p \leqslant P \\ p \equiv l \pmod{Q}}} e^{2\pi i f(p)} \right| \leqslant C_2(k) P L^{-\sigma_0} Q^{-1}.$$

Turán[117] 証明了下面的估計等价于拟似 Riemann 猜想: 当 $3 < |t|^\alpha \leqslant \frac{N}{2} \leqslant N_1 <$ $< N_2 \leqslant N$, $\alpha \geqslant 4$, $0 < \delta \leqslant \frac{1}{2}$ 时,

$$\max_{\frac{t}{10N} \leqslant y \leqslant \frac{3t}{N}} \left| \sum_{N_1 \leqslant p \leqslant N_2} e^{ipy} \right| \ll \frac{N \log^{10} N}{|t|^{\frac{1}{2}+\delta}}.$$

Виноградов[118] 也得到了关于素数变数的特征和的估計, 他在 1952 年得到了下面的結果:

定理 3. 命 q 表一素数, $\chi(n)$ 为 mod q 的非主特征. 若 $q^{\frac{3}{4}} \ll N \ll q^{\frac{5}{4}}$, 則对适合 $k \not\equiv 0 \pmod{q}$ 的任何 k, 都有

$$\sum_{p \leqslant N} \chi(p + k) \ll N^{1+\varepsilon} \left(\frac{q^{\frac{3}{4}}}{N}\right)^{\frac{1}{4}},$$

此处 p 經过 $\leqslant N$ 的全体素数.

由定理 3 立刻得到

定理 4. 命 n 为 $q - 1$ 的一个因子, 且 $1 < n < q - 1$, s 为 $0, 1, 2, \cdots, n-1$ 中的一个; T_s 为适合下面条件的 $p + k$ 的个数:

$$p \leqslant N, \quad \operatorname{ind}(p + k) \equiv s \pmod{n},$$

則在定理 3 的条件下有

$$T_s - \frac{1}{n}\pi(N) \ll N^{1+\varepsilon}\left(\frac{q^{\frac{3}{4}}}{N}\right)^{\frac{1}{4}}.$$

第三章　素数分布及与之相关的 Riemann ζ-函数的性質

16. 素数定理

命 $\pi(x)$ 表示不超过 x 的素数个数. 从 $\pi(x)$ 的最初几个函数值看来, $\pi(x)$ 似乎很不規則, 但是随着数据的增加, 可以看到, 对于函数 $\pi(x)$, 可能有一漸近表示式. Legendre[119] 猜想, 对于充分大的 x, $\pi(x)$ 漸近等于

$$\frac{x}{\log x - 1.08366}, \tag{58}$$

此处 $\log x$ 表示 x 的自然对数. Gauss[120] 又独立地建議了一个类似而并不与它相等的公式. 以一千个連續整数为单位, Gauss 的方法在于計算每个单位中的素数个数, 他建議用函数 $\frac{1}{\log x}$ 来表示在大整数 x 附近的素数分布的平均密度 ("单位区間中素数的百分率"). 因此他用

$$\int_2^x \frac{du}{\log u} \tag{59}$$

来漸近表示 $\pi(x)$. 为了方便起見, 常常用"对数积分"

$$\mathrm{li}\, x = \lim_{\eta\to 0}\left(\int_0^{1-\eta} + \int_{1+\eta}^x\right)\frac{du}{\log u}$$

来代替上面的函数. 这两个函数之差为一常数 $\mathrm{li}\, 2 = 1.04\cdots$. 如果我們仅仅考虑主阶, 則这两个猜想都可以陈述为

$$\lim_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\log x}} = 1. \tag{60}$$

这就是通常所称的"素数定理". 这是素数分布理論中的中心定理. 近百年来, 决定素数定理眞伪的問題, 吸引了不少数学家的注意.

首先在这个方向上作出重要貢献的是 Чебышев[121]. 他在 1848 年与 1850 年証明了

$$a \leqslant \varliminf_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\log x}} \leqslant 1 \leqslant \varlimsup_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\log x}} \leqslant \frac{6}{5}a, \tag{61}$$

此处 $a = 0.92129$. 亦卽他証明了:如果极限存在,则极限必定为 1;而且当 x 充分大时,这个比例界于两个正常数之間. 尽管 Чебышев 所得到的数値上界被以后的数学家不断地加以改进,但这些数学家所用的方法,似乎是不可能导至問題的最終解决的.

Чебышев 引进了两个函数:

$$\vartheta(x) = \sum_{p \leqslant x} \log p \tag{62}$$

及

$$\psi(x) = \sum_{p^m \leqslant x} \log p = \sum_{n \leqslant x} \Lambda(n) = \vartheta(x) + \vartheta(x^{\frac{1}{2}}) + \vartheta(x^{\frac{1}{3}}) + \cdots, \tag{63}$$

此处

$$\Lambda(n) = \begin{cases} \log p, & \text{若 } n \text{ 为素数 } p \text{ 的方冪;} \\ 0, & \text{其他情形.} \end{cases}$$

他証明了下面两个公式都等价于素数定理:

$$\vartheta(x) \sim x \tag{64}$$

与

$$\psi(x) \sim x. \tag{65}$$

最后,我們引征 Sylvester[122] 的話来說明 Чебышев 貢献的意义以及他对这个問題的展望:

"但是要确立这种可能性的存在,我們或許要等待在世界上产生这样一个人,他的智慧与洞察力象 Чебышев 一样,証明自己是超人一等的".

当 Sylvester 写下这些东西的时候,Hadamard 出生了. 但是我們不应該仅仅归功于个别人的才华. 前人的劳动,特别是 Riemann 的工作,为他証明素数定理开辟了道路.

17. Riemann 的解析方法

Riemann[123] 在 1859 年提出的新思想是解决这个問題的鑰匙,他的名著的意义不仅在于素数論,而且亦影响着一般函数論的发展. 他引入了处理复变函数 Riemann ζ-函数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s = \sigma + it, \tag{66}$$

的想法. Euler 在 1737 年将 $\zeta(s)$ 作为实变函数来研究. 他亦得到在素数分布論上的若干应用. 虽然 Riemann 的考虑主要并不在于 $\pi(x)$ 的漸近表示,但他的分析已經明确指出了,在这个函数与 $\zeta(s)$ 的性質間有着密切的联系,特别与它在 s 平面上的零点分布有关. 但是在大多数情况下,Riemann 仅仅只給出了証明的不充分的指示.

为了說明他的名著的价值，我們在这里概述一下他已經証明了的与猜想的結果.

由恆等式

$$\int_0^\infty x^{\frac{1}{2}s-1}e^{-n^2\pi x}\,dx=\frac{\Gamma\left(\frac{1}{2}s\right)}{\pi^{\frac{1}{2}s}}\cdot\frac{1}{n^s}\quad(\sigma>0)$$

出发，我們得到：当 $\sigma>1$ 时，

$$\frac{\Gamma\left(\frac{1}{2}s\right)\zeta(s)}{\pi^{\frac{1}{2}s}}=\sum_{n=1}^\infty\int_0^\infty x^{\frac{1}{2}s-1}e^{-n^2\pi x}\,dx=\int_0^\infty x^{\frac{1}{2}s-1}\psi(x)\,dx$$

成立，此处

$$\psi(x)=\sum_{n=1}^\infty e^{-n^2\pi x}.$$

由于当 $x>0$ 时，$2\psi(x)+1=\frac{1}{\sqrt{x}}\left\{2\psi\left(\frac{1}{x}\right)+1\right\}$，因此

$$\pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\zeta(s)=\int_0^1 x^{\frac{1}{2}s-1}\psi(x)dx+\int_1^\infty x^{\frac{1}{2}s-1}\psi(x)dx=$$

$$=\frac{1}{s(s-1)}+\int_1^\infty\left(x^{-\frac{s}{2}-\frac{1}{2}}+x^{\frac{s}{2}-1}\right)\psi(x)\,dx.\qquad(67)$$

最后的积分对于全体 s 都收斂，故由解析延拓可知，这个公式对于全体 s 都成立. 由于当 s 换为 $1-s$ 时，公式(67)的右端不改变，故得函数方程

$$\zeta(1-s)=\frac{2}{(2\pi)^s}\cos\frac{1}{2}\pi s\Gamma(s)\zeta(s).\qquad(68)$$

由(67)可見，$\zeta(s)$ 除了在 $s=1$ 处有一个殘数为 1 的一次极外，它在整个平面上是正則的. 又因当 $\sigma>1$ 时，

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1},\qquad(69)$$

此处 p 經过全体素数，故当 $\sigma>1$ 时，$\zeta(s)$ 沒有零点. 因此由(68)可知，当 $\sigma<0$ 时，$\zeta(s)$ 除了在 $s=-2,-4,\cdots$ 处有一次零点之外，它沒有其他零点. 我們称这些零点为 $\zeta(s)$ 的“无聊零点”. $\zeta(s)$ 可能有的其他零点 $\rho_1,\rho_2,\cdots$ 都位于带状区域 $0\leqslant\sigma\leqslant1$ 之中. 因为

$$(1-2^{1-s})\zeta(s)=1-\frac{1}{2^s}+\frac{1}{3^s}-\frac{1}{4^s}+\cdots>0\quad(0<s<1)\qquad(70)$$

及 $\zeta(0)\neq0$，所以 $\zeta(s)$ 在 0 与 1 之間的实軸段上沒有零点，亦卽 $\rho_1,\rho_2,\cdots$ 都是复数.

这些就是 Riemann 名著上已經証明了的关于函数 $\zeta(s)$ 的性質. 他还提出了如下的猜想：

1) $\zeta(s)$ 在带状区域 $0 \leqslant \sigma \leqslant 1$ 中有无穷多个零点；

2) 若 $N(T)$ 表示 $\zeta(s)$ 在矩形 $0 \leqslant \sigma \leqslant 1$，$0 < t < T$ 中的零点个数，则

$$N(T) = \frac{1}{2\pi} T \log T - \frac{1 + \log(2\pi)}{2\pi} T + O(\log T);$$

3) 若以 $\rho = \beta + i\gamma$ 来一般标記 $\zeta(s)$ 的非无聊零点，则 $\sum |\rho|^{-2}$ 收斂，而 $\sum |\rho|^{-1}$ 发散；

4) 整函数

$$\xi(s) = \pi^{-\frac{1}{2}s}(s-1)\zeta(s)\Gamma\left(\frac{s}{2}+1\right)$$

可以表为

$$ae^{bs}\prod_{\rho}\left(1-\frac{s}{\rho}\right)e^{\frac{s}{\rho}},$$

此处 $\prod\limits_{\rho}$ 为絕对收斂的无穷乘积，其中 ρ 經过 $\zeta(s)$ 的全体非无聊零点；

5) $\zeta(s)$ 的全体非无聊零点都位于直綫 $\sigma = \frac{1}{2}$ 上；

6) 命 $\Pi(x) = \sum\limits_{2 \leqslant n \leqslant x} \frac{\Lambda(n)}{\log n}$ 及 $\Pi_0(x) = \frac{1}{2}(\Pi(x+0) + \Pi(x-0))$. 則有公式

$$\Pi_0(x) = \mathrm{li}\, x - \sum_{\rho} \mathrm{li}\, x^{\rho} + \int_x^{\infty} \frac{du}{(u^2-1)u \log u} - \log 2 \quad (x > 1),$$

此处 $\mathrm{li}\, x^{\rho} = \mathrm{li}\, e^{\rho \log x}$ 及

$$\mathrm{li}\, e^{w} = \int_{-\infty+vi}^{u+vi} \frac{e^z dz}{z}, \quad w = u + iv, \quad v \gtrless 0.$$

这就是 Riemann 的素数公式.

18. Hadamard 与 von Mangoldt 的貢献

Hadamard[124] 在 1892 年与 1893 年发表了两篇极为重要的整函数論的論文. 他証明了：$\xi(s)$ 是阶等于 1 的整函数，或者更进一步，由 § 17，(67)可以导出 $\xi(s) = O(e^{A|s|\log|s|})$. 因此，Hadamard 在第二篇論文之末解决了 Riemann 的猜想 1)，3)，4). 在 4) 中，我們有 $a = \frac{1}{2}$，$b = \log 2 + \frac{1}{2}\log \pi - 1 - \frac{1}{2}\gamma$，此处 γ 为 Euler 常数. Hadamard[125] 与 de la Vallée Poussin[126] 在 1896 年，几乎同时而又相互独立地証明了素数定理.

von Mangoldt[127] 証明了 Riemann 的另外两个猜想 2) 与 6). 由"幅角原理"可知，$\zeta(s)$（$\xi(s)$ 亦然）在以 $2 \pm iT$ 及 $-1 \pm iT$ 为頂点的矩形中的零点个数 $2N(T)$ 等于

$$\frac{1}{2\pi}[\arg \xi(s)]_C,$$

此处 $[\arg \xi(s)]_C$ 表示当 s 以正向沿矩形的周界 C 走一周时,輻角 $\arg \xi(s)$ 的增加量.显然

$$[\arg \xi(s)]_C = \left[\arg \frac{1}{2} s(s-1)\right]_C + [\arg \Phi(s)]_C,$$

此处 $\Phi(s) = \pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\zeta(s)$. 右端的第一項等于 4π. 又因为 $\Phi(s)$ 在点 s 与点 $1-s$ 处取等值,在点 $\sigma+it$ 及 $\sigma-it$ 处取共軛值,故第二項显然等于 $4[\arg\Phi(s)]_{\mathfrak{L}}$,此处$\mathfrak{L}$ 为由 2 至 $2+iT$ 的綫段 $\mathfrak{L}_1$ 及由$2+iT$ 至 $\frac{1}{2}+iT$ 的綫段 $\mathfrak{L}_2$ 所构成的折綫.因此

$$\pi N(T) = \pi + [\arg \pi^{-\frac{1}{2}s}]_{\mathfrak{L}} + \left[\arg \Gamma\left(\frac{1}{2}s\right)\right]_{\mathfrak{L}} + [\arg \zeta(s)]_{\mathfrak{L}}. \tag{71}$$

首先,我們有

$$[\arg \pi^{-\frac{1}{2}s}]_{\mathfrak{L}} = \left[-\frac{1}{2} t \log \pi\right]_{\mathfrak{L}} = -\frac{1}{2} T \log \pi.$$

其次,由复数形式的 Stirling 公式可知,当 $T \to \infty$ 时,

$$\left[\arg \Gamma\left(\frac{1}{2}s\right)\right]_{\mathfrak{L}} = \Im \log \Gamma\left(\frac{1}{4} + \frac{1}{2}iT\right) - \Im \log \Gamma(1) =$$

$$= \frac{1}{2} T \log \frac{T}{2} - \frac{\pi}{8} - \frac{T}{2} + O(T^{-1}).$$

代入(71)式便得

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + \frac{1}{\pi}[\arg\zeta(s)]_{\mathfrak{L}} + O\left(\frac{1}{T}\right).$$

因此,猜想 2) 的証明就归結为下式的証明:

$$\zeta(T) = \frac{1}{2}[\arg \zeta(s)]_{\mathfrak{L}} = O(\log T).$$

这个公式是下面的关于解析函数的引理的推論. 而这引理本質上是属于 Backlund[128] 的.

引理. 命 $0 \leqslant \alpha < \beta < 2$; $f(s)$ 为一解析函数, 它当 s 为实数时取实值, 又当 $\sigma \geqslant \alpha$ 时,除 $s=1$ 外,为正則的. 又命

$$|\Re f(2+it)| \geqslant m > 0$$

及

$$|f(\sigma'+it')| \leqslant M_{\sigma,t} \quad (\sigma' \geqslant \sigma,\ 1 \leqslant t' \leqslant t).$$

若 T 幷非 $f(s)$ 零点的縱坐标,则当 $\sigma \geqslant \beta$ 时,

$$|\arg f(\sigma+iT)| \leqslant \pi\left(\log M_{\alpha,T+2} + \log\frac{1}{m}\right) \Big/ \log\{(2-\alpha)/(2-\beta)\} + \frac{3\pi}{2}.$$

Backlund 的方法与 von Mangoldt 的証明不一样, 它不依賴于 Hadamard 的供献.

从而也就給 Riemann 的猜想 1）与 3）提供了另一証明．实际上，我們可以得到比 3）更精密的关于零点分布的結果：当 $\alpha > 2$ 时，$\sum|\rho|^{-1}(\log|\rho|)^{-\alpha}$ 收斂，而当 $\alpha \leqslant 2$ 时，这級数发散．并且有

$$\sum_{0<\gamma\leqslant T} \frac{1}{\gamma} = O(\log^2 T) \tag{72}$$

与

$$\sum_{\gamma>T} \frac{1}{\gamma^2} = O\left(\frac{\log T}{T}\right). \tag{73}$$

von Mangoldt 最重要的貢献是他証明了 Riemann 的素数公式（猜想 6））．von Mangoldt 也証明了下面类似的公式．

定理 1. 命 $\psi_0(x) = \frac{1}{2}(\psi(x+0)+\psi(x-0))$．則当 $x>1$ 时，

$$\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log\left(1-\frac{1}{x^2}\right), \tag{74}$$

此处和号 $\sum\limits_\rho$ 表示当 $T\to\infty$ 时，

$$S(x, T) = \sum_{|\gamma|\leqslant T} \frac{x^\rho}{\rho}$$

的极限．

如果将上面的級数逐項积分，便得

定理 2. 当 $x>1$ 时，

$$\psi_1(x) = \int_0^x \psi(t)dt = \frac{1}{2}x^2 - \sum_\rho \frac{x^{\rho+1}}{\rho(\rho+1)} - x\frac{\zeta'}{\zeta}(-1) - \sum_{r=1}^{\infty}\frac{x^{1-2r}}{2r(2r-1)}, \tag{75}$$

此处級数 $\sum\limits_\rho$ 是絕对收斂的．

定理 2 的証明較定理 1 的証明容易，在这里，我們仅仅概述一下（75）式的証明．

先叙述一下 $\zeta(s)$ 的两个性质．

1）存在数貫 $T_2, T_3, \cdots$ 满足

$$m < T_m < m+1, \quad m = 2, 3, \cdots$$

及

$$\frac{\zeta'}{\zeta}(s) \ll \log^2 t \quad (-1 \leqslant \sigma \leqslant 2,\ t = T_m).$$

2）在区域 $\sigma \leqslant -1$，$|s-n| \geqslant \frac{1}{2}$，$n = -2, -4, -6, \cdots$ 中，有

$$\frac{\zeta'}{\zeta}(s) \ll \log(|s|+1).$$

习知

$$\psi_1(x) = -\lim_{m\to\infty}\frac{1}{2\pi i}\int_{2-T_m i}^{2+T_m i}\frac{x^{s+1}}{s(s+1)}\frac{\zeta'}{\zeta}(s)ds.$$

由性质 1) 与 2),将积分直綫 $2+ti(|t|\leqslant T_m)$ 换为折綫:

$$-2m-1\pm ti(|t|\leqslant T_m),\quad \sigma\pm iT_m(-(2m+1)\leqslant\sigma\leqslant 2),$$

在以 $2\pm T_mi$, $-2m-1\pm T_mi$ 为頂点的矩形中,各个殘数之和为

$$\frac{1}{2}x^2-\sum_{|\gamma|<T_m}\frac{x^{\rho+1}}{\rho(\rho+1)}-x\frac{\zeta'}{\zeta}(0)+\frac{\zeta'}{\zeta}(-1)-\sum_{r=1}^{m}\frac{x^{-2r+1}}{(-2r)(-2r+1)}.$$

于是命 $m\to\infty$,便得(75)式.

因此,在 Riemann 的这些猜想中,除猜想 5) 外,都已获得解决. 猜想 5) 就是当今著称的 Riemann 猜想. 从现在开始,所謂 Riemann 猜想就是指猜想 5).

19. 有誤差項的素数定理

素数分布理論的中心問題是寻求

$$\pi(x)-\mathrm{li}\,x$$

或

$$\psi(x)-x$$

的最佳誤差.

在 Riemann 猜想下, von Koch[129] 証明了

$$\psi(x)=x+O(x^{\frac{1}{2}}\log^2 x). \tag{76}$$

事实上,由 § 18, (75)式得到

$$\pm(\psi_1(x\pm 1)-\psi_1(x))=x+O\left(\left|\sum_{\rho}\frac{(x\pm 1)^{\rho+1}-x^{\rho+1}}{\rho(\rho+1)}\right|\right)+O(1)=$$

$$=x+O\left(\sum_{|\rho|\leqslant x}\frac{1}{|\rho|}\left|\int_x^{x\pm 1}u^\rho du\right|\right)+O\left(\sum_{|\rho|>x}\frac{(x+1)^{\frac{3}{2}}}{|\rho(\rho+1)|}\right)=$$

$$=x+O\left(x^{\frac{1}{2}}\sum_{|\gamma|\leqslant x}\frac{1}{|\gamma|}\right)+O\left(x^{\frac{3}{2}}\sum_{|\gamma|>x}\frac{1}{|\gamma|^2}\right)=$$

$$=x+O(x^{\frac{1}{2}}\log^2 x)$$

(其中用到 § 18, (72), (73)式). 因为

$$\psi_1(x)-\psi_1(x-1)=\int_{x-1}^{x}\psi(t)\,dt\leqslant\psi(x)\leqslant\int_x^{x+1}\psi(t)dt=\psi_1(x+1)-\psi_1(x),$$

故得(76)式. 从而也得到

$$\pi(x)=\mathrm{li}\,x+O(x^{1/2}\log x). \tag{77}$$

定理 1. 若 $\zeta(s)$ 在区域

$$\sigma>1-\eta(|t|)$$

中无零点,此处当 $t\geqslant 0$ 时, $\eta(t)$ 为正的递減函数,則

$$\psi_1(x)=\frac{1}{2}x^2+O(x^2e^{-a\omega(x)}),$$

此处 α 为适合 $0<\alpha<1$ 的固定常数，$w(x)=\eta(t)\log x$，而当 $t>0$ 时，t 由等式 $\eta(t)\log x=\log t$ 来定义。

事实上，因为 $x^{-\eta(\gamma)}$ 的递减性及 $x^{-\eta(\gamma)}\leqslant 1$，故由§18，(75)得

$$\psi_1(x)-\frac{1}{2}x^2\ll x^2\left(\sum_{|\gamma|\leqslant T}\frac{1}{|\gamma|^2}x^{-\eta(T)}+\sum_{|\gamma|>T}\frac{x^{-\eta(\gamma)}}{|\gamma|^2}\right)\ll$$

$$\ll x^2\left(x^{-\eta(T)}+\frac{\log T}{T}\right)\ll x^2e^{-\alpha w(x)}. \tag{78}$$

由(78)得

$$\psi(x)=x+O(xe^{-\frac{1}{2}\alpha w(x)}), \tag{79}$$

与

$$\pi(x)=\mathrm{li}\,x+O(xe^{-\frac{1}{2}\alpha w(x)}). \tag{80}$$

Turán[117] 在 $\zeta(s)$ 的无零点区域与 $\pi(x)-\mathrm{li}\,x$ 的阶之間建立了一个紧密关系。

de la Vallée Poussin[130] 証明了：对于

$$\eta(t)=\frac{a}{\log(t+1)},\quad (t\geqslant 1),$$

定理1的假定成立，故得

$$\pi(x)=\mathrm{li}\,x+O(xe^{-a\sqrt{\log x}}). \tag{81}$$

Littlewood[131] 首先引进了估計指数和的方法来改进 $\zeta(s)$ 的无零点区域，从而他証明了可以用較佳的誤差

$$O(xe^{-a\sqrt{\log x\log\log x}})$$

来代替(81)式的誤差。

应用 Виноградов 关于三角和估計的結果，Чудаков[132]，Titchmarsh[133] 及 Виноградов[24] 等人得到了更进一步的結果。最佳的結果为：

定理1的假定对于

$$\eta(t)=\frac{A}{(\log t)^{\frac{2}{3}+\varepsilon}}$$

成立，从而得到

$$\pi(x)=\mathrm{li}\,x+O\,(xe^{-\alpha(\log x)^{\frac{3}{5}+\varepsilon}})^{24)},$$

此处 ε 与 α 为任意給定的正数，而与記号 O 有关的常数仅依賴于 α 及 ε。 Landau 提供了另一个比較初等的、不依賴于 von Mangoldt 公式的处理上述結果的方法。 Rosser[134] 还得到一些数值定理，即

$$\frac{x}{\log x}<\pi(x)<\frac{x}{\log x-2},\quad 若\ 17\leqslant x\leqslant e^{100},\ x\geqslant e^{2000};$$

$$\frac{x}{\log x+2}<\pi(x)<\frac{x}{\log x-4},\quad 若\ x>55;$$

$$p_n>n\log n,\qquad 若\ n\geqslant 1,$$

此处 p_n 表示第 n 个素数。

20. 素数定理誤差項的不規則性

由数値計算可以看出，似乎应該有

$$\pi(x) < \mathrm{li}\, x$$

(見 Ingham[135] 的书)，例如証明了 $\pi(10^9) < \mathrm{li}\, 10^9$。 但是 Littlewood[136] 在 1914 年証明了有充分大的 x，满足 $\pi(x) > \mathrm{li}\, x$，而这样的 x 将要出現无穷多次。 Littlewood 的定理純粹是一个"存在定理"。 以后，Skewes[137] 在 Riemann 猜想下証明了：存在适合 $x < e^{e^{e^{7.703}}}$ 的整数 x，使

$$\pi(x) > \mathrm{li}\, x.$$

在不假定 Riemann 猜想时，他証明了有整数 $x < 10^{10^{10^{10^3}}}$ 也具有此同一性質。

如果存在与 x 无关的正常数 c，使有任意大的 x 满足 $|f(x)| > cx$，则用記号

$$\text{“}f(x) = \Omega(x), \quad (\text{当 } x \to \infty)\text{”}$$

表之。因此"Ω"是"O"的逆記号。 若 $f(x)$ 为实函数，且有任意大的 x 使 $f(x) > cx$，則記为

$$f(x) = \Omega_+(x),$$

又若有任意大的 x，使 $f(x) < -cx$，則記为

$$f(x) = \Omega_-(x).$$

因此"Ω"等价于(对于实函数)"或者 Ω_+，或者 Ω_-"。 用記号"$\Omega_\pm$"表示"Ω_+ 与 Ω_- 的全体"。

Schmidt[138] 証明了，如果在 $\sigma > \Theta > \frac{1}{2}$ 中，$\zeta(s)$ 沒有零点，則对于任意的 $\delta > 0$，有

$$\psi(x) - x = \Omega_\pm(x^{\Theta-\delta})$$

及

$$\pi(x) - \mathrm{li}\, x = \Omega_\pm(x^{\Theta-\delta}).$$

Pólya[139] 得到更精确的結果：命 $w(n)$ 表示在貫 $\psi(1) - 1, \psi(2) - 2, \cdots, \psi(n) - n$ 中出現的变号次数，則

$$\overline{\lim_{n\to\infty}} \frac{w(n)}{\log n} > \frac{c}{\pi},$$

此处 c 的定义如下：若 $\zeta(s)$ 在直綫 $\sigma = \Theta$ 上有零点，则 c 为这些零点的最小正虛部 γ，否則 $c = \infty$。

Littlewood[140] 証明了：当 $x \to \infty$ 时，有

$$\psi(x) - x = \Omega_\pm(x^{\frac{1}{2}} \log\log\log x)$$

与

$$\pi(x) - \mathrm{li}\, x = \Omega_{\pm}\left(\frac{x^{\frac{1}{2}}}{\log x} \log\log\log x\right).$$

21. 相継二素数之差距

設 p_n 是第 n 个素数. 今往研究相継二素数之差距

$$d_n = p_{n+1} - p_n$$

的分布間題. 有两个主要間題:

1) 設法找一函数 $f_1(n)$,使对全体大 n,

$$d_n \ll f_1(n)$$

成立. 在这方面,已知的最优結果本質上属于 Ingham[141],此郎 $f_1(n) = p_n^{\Theta}$, $\Theta = \frac{38}{61} + \varepsilon$.

在 Riemann 猜測成立的假定下, Cramér[142] 証明了 $f_1(n) = p_n^{\frac{1}{2}} \log p_n$. 它的反面間題是去寻找函数 $f_2(n)$,使对无限多个 n,

$$d_n \geqslant f_2(n)$$

成立. 对于这个間題, Rankin[143] 得到了迄今为止的最优結果:

$$f_2(n) = \left(\frac{1}{3} - \varepsilon\right) \log p_n \log\log p_n \frac{\log\log\log\log p_n}{(\log\log\log p_n)^2},$$

他所用的是初等方法.

Western[144] 公布了一张表, 表中包含了这种素数 p_n: $p_n \leqslant 10^7$, 而它們的 d_n 大于一切更小素数之差距. 这种素数一共只有 20 个,其中最大的是 4652353, 在它那里的差距等于 154. 这张表支持了下面的猜測,郎

$$f_1(n) = p_n^{\frac{1}{2}+\varepsilon} \quad 及 \quad f_2(n) = 3(\log_{10} p_n)^2.$$

2) 設法找一函数 $f_3(n)$,使对全体大 n,

$$d_n \geqslant f_3(n)$$

成立. 关于 $f_3(n)$,我們还一无所知;但若有关孿生素数的猜測眞确,就有 $f_3(n) = 2$. 相反地,我們要找一函数 $f_4(n)$,使对无限多个 n,

$$d_n \leqslant f_4(n)$$

成立. Rankin[145] 用 Бухштаб[46] 的方法建立了下面的結果: 对于任何 $\varepsilon > 0$, 都有 $f_4(n) = \left(\frac{57}{59} + \varepsilon\right) \log p_n$;而在广义 Riemann 猜測的假定下,他还証明了 $f_4(n) = \left(\frac{42}{43} \times \times \frac{3}{5} + \varepsilon\right) \log p_n$. Ricci[146] 証明:对于固定的 $\delta(0 < \delta < 1)$,及对充分大的 N, 在区間

$(1-\delta)N < p_n \leqslant N$ 中，至少有千分之五十五的差距 $p_{n+1} - p_n$ 适合不等式

$$p_{n+1} - p_n < \log p_n.$$

另一类問題是去寻找 $f_5(n)$，使对几乎全体 n，

$$d_n \geqslant f_5(n)$$

成立. 所謂"对几乎全体 n 成立"，它的意思是說，适合上述不等式的 $n \leqslant x$ 的个数 $\sim x$.

Walfisz[147] 証明了

$$f_5(n) = \log p_n (\log\log\log p_n)^{-2},$$

而 Prachar[148] 給出了稍更精确的結果：

$$f_5(n) = \frac{\log p_n}{g(p_n)},$$

此处 $g(x)$ 为一在 $x > x_0$（x_0 为一正数）时单調且当 $x \to \infty$ 时适合 $g(x) \to \infty$ 与 $\frac{\log x}{g(x)} \to \infty$ 的函数.

此外，我們还要寻找函数 $f_6(n)$，使

$$d_n \leqslant f_6(n)$$

对几乎全体 n 都成立. 关于这个問題，Cramér[149] 建立了下面的結果：

对于

$$0 \leqslant \alpha < \frac{1}{2}, \quad \beta \geqslant 0, \quad h = x^\alpha (\log x)^\beta,$$

在黎曼猜測眞确的假定下，可有

$$\frac{1}{x} \sum_{\substack{d_n > h \\ p_n \leqslant x}} d_n = O\left(\frac{\log^3 x}{h \log h}\right).$$

由此得到

$$f_6(n) \leqslant (\log n)^3.$$

在此同一假定下，Selberg[150] 証明了：对于 $0 \leqslant \alpha < 1$, $\beta > 0$，可有

$$\frac{1}{x} \sum_{\substack{d_n > \frac{h}{x} p_n \\ p_n \leqslant x}} d_n = O\left(\frac{\log^2 x}{h}\right).$$

由于它的重要性，我們将对 $f_1(n)$ 給出下面的証明过程，Hoheisel[151] 首先証明：有絕对常数 $\Theta < 1$ 存在，使当 $x \to \infty$ 时，

$$\pi(x + x^\Theta) - \pi(x) \sim \frac{x^\Theta}{\log x} \tag{82}$$

成立. 由此得出：当 $n \to \infty$ 时，

$$d_n = O(p_n^\Theta). \tag{83}$$

他的証明能够叙述成下面的一般形式：

我們假定：(a) $\zeta(s)$ 在区域

$$\sigma > 1 - A\frac{\log\log t}{\log t} \quad (A > 0,\ t > t_0 > \xi)$$

中沒有零点；(b) 当 $T \to \infty$ 时，

$$N(\sigma, T) = O(T^{b(1-\sigma)}\log^B T), \quad b > 0,\ B \geqslant 0$$

关于 $\frac{1}{2} \leqslant \sigma \leqslant 1$ 一致地成立，此处 $N(\sigma, T)$ 表示 $\zeta(s)$ 的零点 $\rho = \beta + i\gamma$ 之适合 $\beta \geqslant \sigma$, $0 \leqslant \gamma \leqslant T$ 者之个数．于是，对于满足不等式

$$1 - \frac{1}{b + A^{-1}B} < \Theta < 1$$

的任何固定的 Θ，(82)与(83)都成立。

我們从等式

$$\psi(x) = x - \sum_{|\gamma|<T}\frac{x^\rho}{\rho} + O\left(\frac{x}{T}\log^2 x\right)$$

出发，此式在 $x \to \infty$ 时关于 $3 \leqslant T \leqslant x$ 一致地成立，式中 $\psi(x) = \sum\limits_{p^m \leqslant x}\log p$，而 $\rho = \beta + i\gamma$ 表示 $\zeta(s)$ 的复零点．由此可以得到

$$\psi(x+h) - \psi(x) = h - \sum_{|\gamma|<T}\frac{(x+h)^\rho - x^\rho}{\rho} + O\left(\frac{x}{T}\log^2 x\right),$$

当 $x \to \infty$ 时，記号 O 关于 $3 \leqslant T \leqslant x$, $0 < h \leqslant x$ 为一致的．因为

$$\left|\frac{(x+h)^\rho - x^\rho}{\rho}\right| = \left|\int_x^{x+h} u^{\rho-1}du\right| \leqslant \int_x^{x+h} u^{\beta-1}du \leqslant hx^{\beta-1},$$

故得

$$\frac{\psi(x+h) - \psi(x)}{h} = 1 + O\left(\sum_{|\gamma|<T} x^{\beta-1}\right) + O\left(\frac{x}{Th}\log^2 x\right). \qquad (84)$$

因为 $\zeta(s)$ 只有有限多个适合 $\frac{1}{2} \leqslant \beta < 1$, $|\gamma| \leqslant t_0$ 的零点 $\rho = \beta + i\gamma$，并且它沒有零点适合 $\beta \geqslant 1$，故由假定(a)，一定能够找到 $T_0 > 0$，使在 $T \geqslant T_0$ 与 $\sigma > 1 - \eta(T)$ 中，有 $N(\sigma, T) = 0$，此处 $\eta(T) = A\log\log T/\log T$。

又因 $N\left(\frac{1}{2}, T\right) \gg T\log T$，故若在假定(b)中取 $\sigma = \frac{1}{2}$，可見 $b \geqslant 2$．由 $N(0, T) = O(T\log T)$，我們得到

$$\sum_{|\gamma|<T} x^{\beta-1} = 2x^{-1}N(0, T) + 2\int_0^1 N(\sigma, T)x^{\sigma-1}\log x\,d\sigma \ll$$

$$\ll x^{-1}T\log T + \int_0^{1-\eta(T)}\left(\frac{T^b}{x}\right)^{1-\sigma}\log^B T\log x\,d\sigma,$$

它在 $x\to\infty$ 时关于 $T_0\leqslant T\leqslant x$ 一致地成立.

取 $T=x^{\alpha}$, α 为一适合 $0<\alpha<b^{-1}\left(\leqslant\frac{1}{2}\right)$ 的常数,则得

$$\sum_{|\gamma|<T}x^{\beta-1}=O(x^{\alpha-1}\log x)+O(x^{(\alpha b-1)\eta(x^{\alpha})}\log^{B}x)=O((\log x)^{-\delta}),$$

此处 $\delta=(\alpha^{-1}-b)A-B$. 又取 α 使适合 $\alpha^{-1}>b+A^{-1}B(\geqslant b)$,则有 $\delta>0$,故若 $h=x^{\Theta}$ 而 $1>\Theta>1-\alpha\left(>\frac{1}{2}\right)$,则当 $x\to\infty$ 时,可有

$$\psi(x+h)-\psi(x)\sim h.$$

又因

$$\psi(x+h)-\psi(x)=\sum_{x<p\leqslant x+h}\log p+O\left(\sum_{p^2\leqslant x+h}\log p\left[\frac{\log(x+h)}{\log p}\right]\right)=$$

$$=\sum_{x<p\leqslant x+h}(\log x+O(1))+O\left(\sum_{p^2\leqslant 2x}\log 2x\right)=$$

$$=(\pi(x+h)-\pi(x))(\log x+O(1))+O(x^{\frac{1}{2}}\log x),$$

故前式包含了(82)式,因此也包含了(83)式.

Hoheisel[151] 利用了 Littlewood[131] 的一个定理与 Calson 的某一定理的改进. 前者隐含着有一数值 A 使(a)眞确, 而后者保証(b)对 $b=4$, $B=6$ 成立, 由此他証明了 $\Theta=\frac{32999}{33000}$. Heilbronn[152] 通过增加 A 的数值而将此結果改进到 $\frac{249}{250}$. 借助于 Виноградов 关于指数和的估計, Чудаков[153] 証明了 (a), 其中的 $A=A(t)$ 随 t 趋向无穷, 由此得到 $\Theta=\frac{3}{4}+\varepsilon$. 因此現在的任务在于改进(b). 事实上, Ingham[141] 証明了 $N(\sigma,T)\ll T^{2(1-\sigma)(1+2c)}\log^5 T$,此处 c 为使 $\zeta\left(\frac{1}{2}+it\right)=O(|t|^c)$ 成立的一个正数,也卽(b)对 $b=2(1+2c)$ 与 $B=5$ 眞确. 因此我們得到 $\Theta=\frac{1+4c}{2+4c}+\varepsilon$. 关于 c 的已知最优結果是閔嗣鶴[79] 得到的 $c=\frac{15}{92}+\varepsilon$,由此 $\Theta=\frac{38}{61}+\varepsilon$.

注意, 为了眼下的应用, 关于 $N(\sigma,T)$ 的不等式只在 $\sigma=1$ 的附近才令人感到兴趣. Turán[154] 对 Calson 的公式作出了重要的貢献:对于某一正的数值常数 b,

$$N(\sigma,T)\ll T^{2(1-\sigma)+6(1-\sigma)^{1.1}}$$

在 $1-b\leqslant\sigma\leqslant 1$ 及 $T>3$ 中成立.

此外,如果我們利用 Lindelöf 猜測,也卽对于任何 $\varepsilon>0$, 如果都有 $\zeta\left(\frac{1}{2}+it\right)=$ $=O(|t|^{\varepsilon})$,则有 $\Theta=\frac{1}{2}+\varepsilon$. 在 Riemann 猜測眞确的假定下,我們[141), 142]能够証明

$$p_{n+1}-p_n=O(p_n^{\frac{1}{2}}\log p_n).$$

因若命

$$\Delta_h^{(2)} f(x) = f(x+2h) - 2f(x+h) + f(x),$$

则由 § 18 的定理 2，并用平凡的估計

$$\left|\frac{\Delta_h^{(2)} x^{\rho+1}}{\rho(\rho+1)}\right| \ll \min\left(h^2 x^{-\frac{1}{2}}; \frac{x^{\frac{3}{2}}}{\gamma^2}\right) \quad (1 \leqslant h \leqslant x),$$

可得

$$\Delta_h^{(2)} \psi_1(x) = h^2 + O(x \log^2 x).$$

取 $h = Cx^{\frac{1}{2}} \log x$，$C$ 为充分大的絕对常数，就得到上面的論断.

借助于一个以概率理論为基础的具有启发性的方法[155]，H. Cramér 訊为：对于相継素数之差距，可以猜想它們适合不等式

$$p_{n+1} - p_n \ll (\log p_n)^2.$$

22. 素数在等差級数中的分布

以上各节的大多数結果，都能推广到等差級数中的素数分布問題. 設 $q \geqslant 1$，l 为一适合 $0 < l < q$ 与 $(q, l) = 1$ 的整数. 用 $\pi(x; q, l)$ 表示不大于 x 并且 $\equiv l \pmod q$ 的素数个数，也即

$$\pi(x; q, l) = \sum_{\substack{p \equiv l \pmod q \\ p \leqslant x}} 1.$$

又命

$$\vartheta(x; q, l) = \sum_{\substack{p \equiv l \pmod q \\ p \leqslant x}} \log p$$

及

$$\psi(x; q, l) = \sum_{\substack{n \equiv l \pmod q \\ n \leqslant x}} \Lambda(n).$$

对于 $\sigma > 1$，我們定义函数

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

它有很多性質与 $\zeta(s)$ 的相似.

Чудаков[156] 証明了

$$\psi(x; q, l) = \frac{x}{\varphi(q)} + E(q) \frac{\chi_1(l)}{\varphi(q)\sigma_1} - \frac{1}{\varphi(q)} \sum_{\chi} \bar{\chi}(l) \sum_{|\gamma| \leqslant T} \frac{x^\rho}{\rho} + O\left(\frac{x \log^2 x}{T}\right),$$

这里的 $E(q)$ 或等于 1，或等于 0，完全根据有沒有使 $L(s, \chi_1)$ 在 $\sigma_1 > 1 - \frac{c_1}{\log q}$ 中具有实零点的实特征 $\chi_1(n) \pmod q$ 而定. 又 $\rho = \beta + i\gamma$ 表示 $L(s, \chi)$ 的零点，而含在記号 O 中的常数则与 q 无关.

如果有模 q 特征的全体 Dirichlet L-函数在区域

$$\sigma > 1 - \frac{A}{\log(|t|+2)^{\frac{2}{3}}}$$

中都沒有零点，则用 § 19 中的方法，我們得到

$$\psi(x;\ q,\ l) = \frac{1}{\varphi(q)}x + O\left(xe^{-c(\log x)^{\frac{3}{5}-\varepsilon}}\right),$$

記号 O 中所含的常数与 q 及 ε 有关．我們也能証明

$$\pi(x;\ q,\ l) = \frac{1}{\varphi(q)}\operatorname{li} x + O\left(xe^{-c(\log x)^{\frac{3}{5}}}\right)$$

及

$$p_{n+1} - p_n = O\left(p_n^{\frac{38}{61}+\varepsilon}\right),$$

此处 p_n 表等差級数 $\equiv l \pmod q$ 中的第 n 个素数．

我們也能得到一个关于 q 为一致的結果．实际上，Page[157] 証明了：(a) $L(s,\chi)$ 在

$$t \geqslant 3,\quad \sigma > 1 - \frac{a_2}{\log qt}$$

中沒有零点；(b) 对于任何复特征 χ，$L(s,\chi)$ 在 $\sigma \geqslant 1 - \frac{a_3}{\log q}$，$|t| \leqslant 5$ 中沒有零点；(c) $L(s,\chi)$ 在

$$\sigma \geqslant 1 - \frac{a_4}{\log q},\quad 0 < t < 5$$

中沒有零点；(d) 設 $\xi \geqslant 2$，在由以 $q(\leqslant \xi)$ 为模的实原特征所构成的全体 L-函数中，至多有一函数，它有一实零点适合 $\sigma > 1 - \frac{a_5}{\log \xi}$．利用这些結果，我們导得

$$\pi(x;\ q,\ l) = \frac{1}{\varphi(q)}\operatorname{li} x + O\left(xe^{-c(\log x)^{\frac{1}{2}}}\right) + O\left(\frac{x^{\sigma_1}}{\varphi(q)\log x}\right),$$

此处 σ_1 为模 q 的 L-函数所具有的最大实零点，而 c 为一正常数． Tatuzawa[158] 对此公式作了某种改进．

有沒有可能把第二个誤差項除去？ 它的困难点在于有实特征的 L-函数的实零点的分布情形．以后在 C. L. Siegel[159] 关于二次型类数的 Gauss 問題的极为重要的工作中，这个困难被克服了．他証明了：对于任何給定的 $\varepsilon > 0$，存在数 A，使在 $\sigma > 1 - q^{-\varepsilon}$ 与 $q > A$ 中，有

$$L(\sigma,\chi) \neq 0.$$

通过将 Page 与 Siegel 的結果的結合，Walfisz[160] 建立了下面的重要定理：設 $q \geqslant$ $\geqslant 3$，又 $q \leqslant (\log x)^h$ 而 $h \geqslant 1$，則有

$$\pi(x;q,l)=\frac{1}{\varphi(q)}\operatorname{li}x+O(xe^{-c(\log x)^{\frac{1}{2}}}),\tag{85}$$

記号 O 中所含的常数与 q 无关.

虽然这个公式远优于 Page 的結果,但在它的証明中,还有一点不足之处. 因为 Siegel 的定理只是一个存在性定理, 我們无法通过有限的步驟来找出(85)中的显常数. 例如,如果用(85)去証明 Виноградов 的"三素数定理",我們就无法定出奇素数究竟需要大到怎样程度才能表成三个素数的和. 但是我們能够避开 Siegel 定理, 而用 Page 原来的工作,来証明具有确定数值常数的"三素数定理".

关于等差級数中的素数分布, 另一个有趣問題是为等差級数 $\equiv l \pmod q$ 中的最小素数 $p(q,l)$ 找一上界. Линник[161] 开辟了重要的一步. 他証明了: 这种素数一定是 $O(q^c)$, c 为一絕对常数. 以后, Родосский[162] 簡化了他的証明. S. Chowla[163] 猜测:对于任何 $\varepsilon>0$ 及对全体大 q, $\equiv l \pmod q$的最小素数一定不大于 $q^{1+\varepsilon}$; Turán[164] 証明: 如果广义黎曼猜想成立, 那末 Chowla 的猜想对几乎全体模 q 的等差級数都眞确. 另一方面, Erdös[165] 証明了: (a) 存在常数 $c_2=c_2(c_1)$ 与无穷多个整数 q,使

$$p(q,l)>(1+c_1)\varphi(q)\log q$$

对不少于 $c_2\varphi(q)$ 个 l 值成立; (b) 存在常数 $c_4=c_4(c_3)$,使

$$p(q,l)\leqslant c_3\varphi(q)\log q$$

对 $c_4\varphi(q)$ 个 l 值成立.

23. 其他素数問題

設 $\pi_\nu(x;q,l)$ 为不大于 x 并且是 ν 个素数的乘积,同时又是 $\equiv l \pmod q$ 的整数的个数. Richert[166] 証明了:

$$\pi_\nu(x;q,l)=\frac{1}{\varphi(q)}\sum_{0\leqslant m\leqslant\frac{1}{c}\sqrt{\log x}}\ \sum_{0\leqslant h\leqslant\nu-1}A_\nu(h,m,q)\int_2^x\frac{(\log\log u)^h}{(\log u)^{m+1}}du+$$

$$+O(xe^{-\frac{1}{c}\sqrt{\log x}})+O\left(x^{1-\frac{1}{bq^\varepsilon}}\frac{\log^{\nu-1}q(\log\log x)^{\nu-1}}{\varphi(q)\log x}\right),$$

这里的 b 为一与 ε 有关的数, c $(\geqslant 20)$ 为一常数, $A_\nu(h,m,q)$ 通过一个只与 h, m, q 及 ν 有关的級数而定义.

И. И. Пятецкий-Шапиро[167] 証明了:对于 $1\leqslant c<\frac{12}{11}$,在序列 $[n^c]$ 中不大于 x 的素数个数与 $\frac{x^{\frac{1}{c}}}{\log x}$ 漸近相等.

Landau[168] 将素数分布理論方面的古典結果推广到任何代数数域.

設 k 为一 n 次代数数域，$\pi_k(x)$ 为有距 $\leqslant x$ 的素理想数的个数，則有

$$\pi_k(x) = \mathrm{li}\, x + O\left(xe^{-\frac{a}{\sqrt{n}}\sqrt{\log x}}\right),$$

$$\vartheta_k(x) = \sum_{N\mathfrak{p}\leqslant x} \log N\mathfrak{p} = x + O\left(xe^{-\frac{a}{\sqrt{n}}\sqrt{\log x}}\right),$$

此处 a 为一絕对常数，又有

$$\pi_k(x) - \mathrm{li}\, x = \Omega_{\pm}\frac{\sqrt{x}}{\log x}\log\log\log x.$$

对于类中的理想数也有类似的結果.

24. 素因子有某种特殊性质的整数的分布

命 $\Phi(x, y)$ 表示 $\leqslant x$ 且无素因子 $< y$ 的自然数的个数. Бухштаб[169] 証明了

$$\Phi(y^u, y) = w(u)\frac{y^u}{\log y} + O\left(\frac{y^u}{(\log^u y)^{\frac{3}{2}}}\right), \tag{86}$$

記号 O 中所含的常数与 u 无关，并且

$$\left.\begin{aligned} w(u) &= \frac{1}{u} \quad (1 \leqslant u \leqslant 2), \\ (uw(u))' &= w(u-1) \quad (u > 2). \end{aligned}\right\} \tag{87}$$

命 $\psi(x, y)$ 表示 $\leqslant x$ 且无素因子 $> y$ 的自然数的个数，則有

$$\psi(y^u, y) = \rho(u)y^u + O\left(\frac{y^u}{(\log y)^{\frac{1}{2}}}\right), \tag{88}$$

此处

$$\left.\begin{aligned} \rho(u) &= 1 \qquad (0 < u \leqslant 1), \\ u\rho'(u) &= -\rho(u-1) \quad (u > 1). \end{aligned}\right\} \tag{89}$$

[170), 171)]

函数

$$f(s) = \int_0^\infty e^{-su} dw(u+1)$$

滿足下之微分方程:

$$f'(s) + (s^{-1}(e^{-s} - 1) - 1)f(s) = s^{-1}(1 - e^{-s}).$$

解此方程，并因

$$\lim_{s=\infty} f(s) = 0,$$

故得

$$f(s) = -1 - se^s + e^{-\gamma + s + \int_0^s t^{-1}(1 - e^{-t})dt}.$$

命 $s \to 0$，則有

$$-1+e^{-\gamma}=\lim_{s\to 0} f(s)=\lim_{s\to 0}\int_0^\infty e^{-us}dw(u+1)=\int_0^\infty dw(u+1)=w(\infty)-w(1),$$

也即

$$\lim_{u\to\infty} w(u)=e^{-\gamma}. \tag{90}$$

因为

$$w(u)-e^{-\gamma}=-\int_u^\infty w'(t)dt$$

及

$$w'(u)=-\frac{1}{u}\int_{u-1}^{u} w'(t)dt,$$

故由下面的初等引理,我們得到

$$w'(u)<e^{-u\left(\log u+\log\log u-\frac{\log\log u}{\log u}+O\left(\frac{1}{\log u}\right)\right)}$$

及

$$|w(u)-e^{-\gamma}|<e^{-u\left(\log u+\log\log u-\frac{\log\log u}{\log u}+O\left(\frac{1}{\log u}\right)\right)}. \tag{91}$$

引. 設 $F(u)$ 为在 $u>0$ 时定义的一个正値函数,又对充分大的 u, $F(u)$ 适合不等式

$$F(u)\leqslant\frac{1}{u}\int_0^1 F(u-1+\vartheta)d\vartheta,$$

則有

$$F(u)\leqslant e^{-u\left(\log u+\log\log u-1+\frac{\log\log u}{\log u}+O\left(\frac{1}{\log u}\right)\right)}.$$

类似地,我們能够証明

$$\rho(u)=e^{-u\left(\log u+\log\log u-1+\frac{\log\log u}{\log u}\right)+O\left(\frac{u}{\log u}\right)}\text{[172),173),174),175)]}. \tag{92}$$

De Bruijn 引进了函数 Λ:

$$\Lambda(y^u,y)=y^u\int_0^\infty \rho\left(\frac{u\log y-\log t}{\log y}\right)d\frac{[t]}{t},$$

并以此代替(88)中的 $y^u\rho(u)$,从而証得了

$$\psi(y^u,y)=\Lambda(y^u,y)+O(u^2y^uR(y))\text{[176)]}, \tag{93}$$

式中 $R(y)$ 的阶大体上为 $\dfrac{|\pi(y)-\mathrm{li}\,y|}{y}$.

本节的結果可以推广到一个給定的等差級数中.

第四章　Waring 問題

25. 解析方法的引进

設 k 与 N 都是自然数，命 $P=[N^{\frac{1}{k}}]$，又命

$$T(\alpha)=\sum_{x=1}^{P}e^{2\pi i\alpha x^k},$$

則

$$r_s(N)=\int_0^1(T(\alpha))^s e^{-2\pi iN\alpha}\,d\alpha=\int_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}}(T(\alpha))^s e^{-2\pi iN\alpha}d\alpha \tag{94}$$

就是不定方程

$$x_1^k+x_2^k+\cdots+x_s^k=N,\quad x_i\geqslant 1 \tag{95}$$

的解数，此处 $\tau=2kP^{k-1}$.

用 $\mathfrak{M}_{h,q}$ 表示区間

$$\left|\alpha-\frac{h}{q}\right|\leqslant\frac{1}{q\tau},\quad (h,q)=1,\quad q\leqslant P^{\beta},$$

此处 $\frac{1}{4}\leqslant\beta\leqslant 1-\frac{1}{k}$. 今往估計 $\mathfrak{M}_{h,q}$ 上的 $T(\alpha)$. 置 $x=qy+r$ 及 $\alpha=\frac{h}{q}+\vartheta$，則有

$$T(\alpha)=\sum_{r=1}^{q}e^{2\pi ihr^k/q}\sum_{0<qy+r\leqslant P}e^{2\pi i(qy+r)^k\vartheta}.$$

命 $f(y)=\vartheta(qy+r)^k$，因为

$$|f'(y)|=|k\vartheta(qy+r)^{k-1}q|<\frac{kP^{k-1}q}{2kqP^{k-1}}=\frac{1}{2},$$

故按 §8 引理 1 可得

$$T(\alpha)=\sum_{r=1}^{q}e^{2\pi ihr^k/q}\int_{0<qt+r\leqslant P}e^{2\pi i(qt+r)^k\vartheta}dt+O(q)=$$

$$=\frac{1}{q}\sum_{r=1}^{q}e^{2\pi ihr^k/q}\int_0^P e^{2\pi ix^k\vartheta}dx+O(q).$$

借助于下面两个估計:

$$\sum_{r=1}^{q}e^{2\pi ihr^k/q}=O(q^{1-\frac{1}{k}}),\quad \int_0^P e^{2\pi ix^k\vartheta}\,dx=O\left(\min\left(P,|\vartheta|^{-\frac{1}{k}}\right)\right),$$

我們得出

$$\int_{\mathfrak{M}_{h,q}}(T(\alpha))^s e^{-2\pi i\alpha N}d\alpha=\frac{1}{q^s}\left(\sum_{r=1}^{q}e^{2\pi ihr^k/q}\right)^s e^{-2\pi ihN/q}\times$$

$$\times\int_{-\infty}^{+\infty}\left(\int_0^P e^{2\pi ix^k\vartheta}dx\right)^s e^{-2\pi iN\vartheta}d\vartheta+O\left(\frac{P^{s-k-1}}{q}\right)+O\left(\frac{P^{s-k-\frac{1}{k}}}{q^{2+\frac{1}{k}}}\right).$$

最后，对于 $s\geqslant 2k+1$，我們得到

$$\sum_{\mathfrak{M}_{h,q}}\int_{\mathfrak{M}_{h,q}}(T(\alpha))^s e^{-2\pi i\alpha N}d\alpha=\mathfrak{S}(N)N^{\frac{s}{k}-1}\frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}+O(P^{s-k-\frac{1}{k}}),$$

此处

$$\mathfrak{S}(N)=\sum_{q=1}^{\infty}\sum_{\substack{h=1\\(h,q)=1}}^{q}\left(\frac{1}{q}\sum_{x=1}^{q}e^{2\pi ihx^k/q}\right)^s e^{-2\pi iNh/q}.$$

对于 $s\geqslant 4k$，我們能够証明

$$\mathfrak{S}(N)\gg 1.$$

于是問題化为去估計积分(94)在 E 上的部分，E 是不属于任何 $\mathfrak{M}_{h,q}$ 的点的集合. 如果它的阶等于 $o(P^{s-k})$，則对大 N，将有 $r_s(N)>0$.

积分的剩余部分的处理依賴于下面两个估計：由第二章，§7 得出的

$$\max_{\alpha\in E}|T(\alpha)|\ll P^{1-2^{1-k}+\varepsilon}\tag{96}$$

及

$$\int_0^1|T(\alpha)|^{2^k}d\alpha\ll P^{2^k-k+\varepsilon}.\tag{97}$$

于是对于 $s>2^k$，可有[177]

$$r_s(N)=\int_0^1(T(\alpha))^s e^{-2\pi iN\alpha}d\alpha\sim\mathfrak{S}(N)N^{\frac{s}{k}-1}\frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}.\tag{98}$$

Виноградов[27] 用另外两个估計代替(96)及(97)，它們是

$$\max_{\alpha\in E}|T(\alpha)|\ll P^{1-\frac{1}{2k^2(2\log k+\log\log k+3)}+\varepsilon},\tag{99}$$

以及对 $t\geqslant\frac{1}{4}k(k+1)+lk$，$0\leqslant l\leqslant c_1(k)$ 成立的

$$\int_0^1|T(\alpha)|^{2t}d\alpha\ll P^{2t-k+\delta}(\log P)^{2l},\tag{100}$$

此处

$$\delta=\frac{1}{2}\left(1-\frac{1}{k}\right)^l k(k+1)$$

(它由 §9 定理 1 导出). 于是对于

$$s \geqslant 2k^2(2\log k + \log\log k + 2.5)^{178)}$$

与 $k > 10$, (98)式成立.

Hardy–Littlewood 曾經猜測

$$\sum_{n=1}^{N} r_k^2(n) = O(N^{1+\varepsilon})$$

成立,或者与它等价的有

$$\int_0^1 |T(\alpha)|^{2k} d\alpha \ll P^{k+\varepsilon}.$$

假如这个猜測眞确, 那末容易看到, 上面的漸近公式对于 $s \geqslant 2k+1$ 成立. 但除在 $k = 2$ 时外,这个猜測之为正确或为錯誤, 至今还未能够确定. 由此猜測.我們立刻推得:除在 $k = 2^m$ 而 $m > 1$ 时外,都有

$$G(k) \leqslant 2k + 1,$$

而在这些例外情形中, $G(k) = 4k$. $G(k)$ 的意义将在 §26 中給出.

假如

$$r_k(n) = O(n^\varepsilon),$$

則 Hardy–Littlewood 的猜測就能成立. 但另一方面, Erdös[179], Chowla 与 Pillai[180] 証明了

$$r_k(n) = \Omega(e^{c\log n/\log\log n}).$$

对于 $k = 3$ 的情形, Mahler[181] 証明

$$x^3 + y^3 + z^3 = n^{12}$$

的解数 $\gg n$.

26. $G(k)$ 的上界

命 $G(k)$ 为使

$$x_1^k + \cdots + x_s^k = N, \quad x_\nu \geqslant 0 \tag{101}$$

对全体充分大的 N 都有整数解 x_ν 的最小整数 s. 上节的結果不仅告訴我們

$$G(k) \leqslant \begin{cases} 2^k + 1 & (k \leqslant 10), \\ 2k^2(2\log k + \log\log k + 2.5) & (k > 10); \end{cases}$$

并且还給出了(101)的解数的漸近公式. 如果我們无意保住此漸近公式,我們便能得到 $G(k)$的一个更好的上界.下述方法属于 Виноградов,它以下面的引理作为出发点.

引 1 (Hardy–Littlewood). 命

$$P_1 = \left[\frac{1}{4}P\right], \quad P_2 = \left[\frac{1}{2}P_1^{1-\frac{1}{k}}\right], \quad \cdots, \quad P_m = \left[\frac{1}{2}P_{m-1}^{1-\frac{1}{k}}\right],$$

又命 $\xi_i (i = 1, 2, \cdots, m)$ 經过区間

$$P_i \leqslant \xi_i < 2P_i$$

中的整数,则对固定的 m 与对充分大的 P,数

$$u = \xi_1^k + \cdots + \xi_m^k$$

各各不同,并且都在 $\left(\frac{1}{5}P\right)^k$ 与 $\left(\frac{1}{2}P\right)^k$ 之間. 又設 $P_m \leqslant \xi_m' < 2P_m$, 則对任何 $\varepsilon > 0$ 及对給定的 v,方程

$$v = \xi_1^k + \cdots + \xi_m^k + \xi_m'^k$$

的解数等于 $O(v^\varepsilon)$. 这种 v 的个数 $\gtrless P^{k-(k-2)\left(1-\frac{1}{k}\right)^{m-1}}$.

引理的第一部分由下之事实,即由

$$(\xi_1 + 1)^k - \xi_1^k \geqslant k\xi_1^{k-1} \geqslant kP_1^{k-1} > (2P_2)^k + \cdots + (2P_m)^k > \xi_2^k + \cdots + \xi_m^k$$

导出. 引理的第二部分还需要另外一个結果,即 $\xi_m^k + \xi_m'^k = w$ 的解数等于 $O(w^\varepsilon)$.

命

$$T_{i-1}(\alpha) = \sum_{\xi_i} e^{2\pi i \xi_i^k \alpha},$$

$$Q(\alpha) = T_1(\alpha) \cdots T_m(\alpha) T_{m+1}^2(\alpha)$$

及

$$R(\alpha) = T_0(\alpha) Q(\alpha).$$

引理告訴我們,

$$\int_0^1 |R(\alpha)|^2 d\alpha \ll R(0) P^\varepsilon.$$

命

$$b = \begin{cases} 2k^2(2\log k + \log\log k + 3) & (k > 12), \\ 2^{k-1} & (k \leqslant 12) \end{cases} \tag{102}$$

及

$$m = \left[\frac{\log \frac{1}{2} b + \log \frac{(k-2)}{\left(k - \frac{1}{2}\right)}}{-\log\left(1 - \frac{1}{k}\right)} \right], \tag{103}$$

則在 E 上可有

$$\int_E |T_0^{2k-1}(\alpha) R^2(\alpha)| d\alpha \ll \max_{\alpha \in E} |T_0(\alpha)|^{2k-1} \int_0^1 |R(\alpha)|^2 d\alpha \ll$$

$$\ll P^{\left(1-\frac{1}{b}\right)(2k-1)+\varepsilon} R(0) = o(P^{k+1} Q^2(0)),$$

这是因为

$$(k-2)\left(1 - \frac{1}{k}\right)^{m+1} < \frac{2k-1}{b}$$

的原故．又不难証明

$$\sum_{\mathfrak{M}_{h,q}}\int_{\mathfrak{M}_{h,q}} T_0^{2k-1}(\alpha)R^2(\alpha)e^{-2\pi i\alpha N}d\alpha \gg P^{k+1}Q^2(0).$$

于是因为 $m \sim 2k\log k$，所以我們建立了

$$G(k) \leqslant 2k + 2m + 5 \sim 4k\log k.$$

这个結果又被 Виноградов[27] 进一步改进为：对于 $k \geqslant 3$，有

$$G(k) < 3k(\log k + 9).$$

証明依赖于下面的

引 2. 設

$$U(\alpha) = \sum_p \sum_{u_0} e^{2\pi i\alpha p^k u_0},$$

此处 u_0 經过引理 1 中給出的整数集合，但以 $[P^{\frac{1}{2}}]$ 代替 P 与以 m_0 代替 m，又 p 經过区間 $\frac{1}{2}[P^{\frac{1}{2}}] \leqslant p \leqslant [P^{\frac{1}{2}}]$ 中的全体素数．于是当 $\alpha \in E$ 时，有

$$U(\alpha) \ll U(0)P^{-\frac{1}{8}+\frac{k}{4}\left(1-\frac{1}{k}\right)^{m_0}+\varepsilon}.$$

我們选取 m_0 与 m 为使

$$k\left(1-\frac{1}{k}\right)^{m_0-1} < \frac{1}{6} \quad 与 \quad k\left(1-\frac{1}{k}\right)^m < \frac{1}{12}$$

成立的最小整数，亦即

$$m_0 = \left[\frac{\log 6k}{-\log\left(1-\frac{1}{k}\right)} + 2\right] \quad 与 \quad m = \left[\frac{\log 2k}{-\log\left(1-\frac{1}{k}\right)} + 1\right],$$

則因

$$|T(\alpha)| = \left|\sum_{x=1}^{P} e^{2\pi i x^k\alpha}\right| \leqslant P,$$

故得

$$\int_E T(\alpha)^{2k+1}R^2(\alpha)U(\alpha)d\alpha \ll P^{2k+1}\max_{\alpha\in E}|U(\alpha)|\int_0^1 |R(\alpha)|^2 d\alpha \ll$$
$$\ll P^{2k+1}U(0)P^{-\frac{1}{8}+\frac{1}{24}\left(1-\frac{1}{k}\right)+\varepsilon}R(0) \ll$$
$$\ll P^{2k+1}U(0)R^2(0)P^{-k-\frac{1}{24k}}.$$

于是我們能够証明：当 $P \to \infty$ 时，有

$$\int_0^1 T(\alpha)^{2k+1}R^2(\alpha)U(\alpha)e^{-2\pi i\alpha N}d\alpha \sim cT(0)^{k+1}R^2(0)U(0)$$

与 $c > 0$．由此得出：对于 $k \geqslant 3$，有

$$G(k) \leqslant 2k + 1 + m_0 + 2m < 3k(\log k + 3).$$

Davenport[28] 改进了引 1,从而能够証明: $G(4)=16$ (一个变化了的数: $G^*(4)\leqslant$ $\leqslant 14$), $G(5)\leqslant 23$, $G(6)\leqslant 36$, $G(7)\leqslant 52$, $G(8)\leqslant 73$.

Линник[29] 証明了: $G(3)\leqslant 7$. (另有一个簡单証明,請見 Watson[182]).

我們可以通过两个不同的方法来証明 $G(k)$ 的下界 $\geqslant k+1$:

a) 能够表成

$$x_1^k+\cdots+x_k^k,\quad x_\nu\geqslant 0$$

形状的 $n(\leqslant N)$ 的个数少于滿足条件

$$0\leqslant x_1\leqslant x_2\leqslant\cdots\leqslant x_k\leqslant[N^{\frac{1}{k}}]$$

的 $x_1,\cdots,x_k$ 的組数. 显然,对于充分大的 N, 后者 $<\frac{2}{3}N$.

b) 关于同余式的考慮.

直到 1909 年为止,这个由 Waring[4] 提出的問題只在不多的数值結果中显示出微小的苗头. 1909 年, Hilbert[5] 証明了:对于每一 k, $G(k)$ 都存在. 他先用一个 25 重的重积分証明了下面的事实:对于每一 k, 都存在一个有五个变元 $x_1,\cdots,x_5$ 的形状如

$$(x_1^2+\cdots+x_5^2)^k=\sum_h r_h(a_{1h}x_1+\cdots+a_{5h}x_5)^{2k}$$

的恆等式,其中 a_{ih} 都是整数,而 r_h 则是正有理数. 这是在証明关于 $k=2^m(m=1, 2,\cdots)$ 的 Waring 定理过程中的一个步驟. 任意指数的情形能够由此通过一个冗长的研究而得出.

虽然 Hilbert 的証明被很多数学家[183]所簡化,但由此方法得到的 $G(k)$仍然过大.

Hardy 与 Littlewood 在 1920—1928 年出版的总标題为 "partitio numerorum" 的一系列工作中,展开了一个重要的研究 Waring 問題的解析方法. 但关于 $G(k)$ 上界的最重要的改进,还是 Виноградов 得到的. 他引进了数論中的一个強有力的方法,即三角和方法.

27. Waring 問題的各种推廣

設 $f(x)$ 为一 k 次整值多項式. 前述的大多数結果,除开 $G(3)\leqslant 7$ 与 $G(k)<$ $<k(3\log k+9)$外,都能推广到多項式的情形. 华罗庚[93),184] 克服了其中的主要困难. 例如,我們能够証明:对于 $k\leqslant 10$ 而 $s\geqslant 2^k+1$, 以及对于 $k>10$ 而 $s\geqslant 2k^2(2\log k+$ $+\log\log k+2.5)$, 关于

$$N=f(x_1)+\cdots+f(x_s)\tag{104}$$

的解数,有一漸近公式. 又

$$N=f_1(x_1)+\cdots+f_s(x_s)$$

的問題[177),185)]也如此。

設

$$f(x)=a_k\binom{x}{k}+a_{k-1}\binom{x}{k-1}+\cdots+a_1\binom{x}{1}$$

及

$$(a_k, a_{k-1}, \cdots, a_1)=1,$$

此处 $\binom{x}{r}=\frac{x(x-1)\cdots(x-r+1)}{r!}$. 我們定义 $G(f)$ 为使方程(104)对全体充分大的 N 都可解的最小整数 s. 华罗庚[186)]証明了

$$G(k\text{ 次多項式})\leqslant(k-1)2^{k+1}$$

与[187)]

$$G(3\text{ 次多項式})\leqslant 8.$$

Нечаев[188)]証明

$$G\left(\left(\binom{x}{k}\right)\right)<4k\log k+8k\log\log k.$$

又华罗庚[186)]指出

$$\max_{f(x)} G(f)\geqslant 2^k-1,$$

这里的 $f(x)$ 經过全体 $k(\geqslant 5)$ 次整值多項式。

命 $G^*(f(x))$ 表示使

$$f(x_1)+\cdots+f(x_s)=N$$

在

$$f(x_1)+\cdots+f(x_s)\equiv N\ (\mathrm{mod}\ q)$$

对任何 q 都可解时为可解的最小整数 s,則有[189)]

$$G^*(f(x))\leqslant 2m+2k+5\sim 4k\log k,$$

m 的定义見第四章 § 26 中的(102)与(103). 又依靠 Davenport 引理的帮助，还能得到一些特殊結果，例如，

$$G^*(\text{四次多項式})\leqslant 14,$$

$$G^*(\text{五次多項式})\leqslant 23.$$

Roth[190)]証明：每一充分大的整数都能表成 $x_1^2+x_2^3+\cdots+x_{50}^{51}$ 的形式，$x_i\ (i==1, 2, \cdots, 50)$ 都是正整数. 他还証明：几乎全体正整数 n 都能表成

$$x_1^2+x_2^3+x_3^4+x_4^5$$

的形状。

Wright[191)]在变量上添加了阶的条件，他証明了：設 $\lambda_1, \cdots, \lambda_s$ 都是正数，并且

$\sum_{\nu=1}^{s} \lambda_\nu = 1$,又設 $k \geqslant 3$,而

$$s \geqslant (k-2)2^{k-1} + 5,$$

則每一充分大的整数 n 都能表成 s 个正的 k 次乘冪的和,如

$$n = m_1^k + \cdots + m_s^k,$$

并且这些 m 适合

$$|\lambda_i n - m_i^k| = O(n^{1-\beta}), \quad i = 1, 2, \cdots, s.$$

此处 $0 < \beta < \alpha$,而 α 为 k 与 s 的某一函数. 例如,若 $k=3$ 与 $s=9$,則 $\alpha = \frac{1}{51}$. 如果用 Виноградов 的方法,这个結果肯定还能改进.

对于 $n \not\equiv 0 \pmod 8$ 的情形, Auluck 与 Chowla[192] 証明: n 能够表成

$$n = m_1^2 + \cdots + m_4^2$$

的形状,此处

$$\frac{n}{4} - m_i^2 = O(n^{\frac{3}{4}}).$$

命 $c > 1$, 但非整数. Сегал[193] 曾經研究用形如

$$x_1^c + x_2^c + \cdots + x_s^c$$

的表示式来近似表示数的問題,这里的 x_i 都是正整数. Сегал[193] 証明了: 存在 $s_0(c)$, 使当 $s \geqslant s_0(c)$ 时,不等式

$$\left| \sum_{i=1}^{s} x_i^c - N \right| < \Delta_N$$

为可解,这里的 Δ_N 在 N 趋向无穷时趋于零.

另外还有一些問題,它們在某些方面与 Waring 問題相似. 例如, 定出 s 的下界 $s_0(k)$,使不等式

$$\left| \sum_{i=1}^{s} \lambda_i x_i^k \right| < \varepsilon \tag{105}$$

对任何 $\varepsilon > 0$ 与 $s \geqslant s_0(k)$ 都有正整数解 x_i. 显然, 这些 λ 不能有相同的符号. Chowla[194] 証明:如果比数 λ_s/λ_t $(s \neq t)$ 都是无理数,則 $s_0(2) \leqslant 9$.

利用 Hardy-Littlewood 方法的一个变形, Davenport 与 Heilbronn[195] 証明了: 如果至少有一比数 λ_s/λ_t $(s \neq t)$ 为无理数,則有 $s_0(2) \leqslant 5$. 在此同一条件下, Davenport 与 Roth[196] 討論了 $k = 3$ 的情形,他們証明了 $s_0(3) \leqslant 8$. 另外他們用 Виноградов 处理 Waring 問題的方法証明了:存在絕对常数 c,使对 $k \geqslant 12$,有

$$s_0(k) \leqslant ck \log k.$$

关于下述問題的研究,請見 Oppenheim[197]. 这个問題是, 确定 s 的下界 s_0, 使不

等式

$$0 < f(x_1, \cdots, x_s) < \varepsilon$$

对任何 $\varepsilon > 0$ 都有整数解 x_i,此处 f 为一具实系数的不定二次型.

28. $g(k)$ 的上界

用 $g(k)$ 表示使

$$N = x_1^k + \cdots + x_s^k, \quad x_i \geqslant 0$$

对全体整数 $N \geqslant 0$ 都可解的最小整数 s. 命 $q = \left[\left(\frac{3}{2}\right)^k\right]$, 数

$$n = 2^k q - 1 < 3^k$$

只可能用 1^k 与 2^k 表出. 因为

$$n = (q-1)2^k + (2^k - 1) \cdot 1^k,$$

故在 n 的表示中正巧需要

$$q - 1 + 2^k - 1 = 2^k + q - 2$$

个 k 次乘幂. 因此

$$g(k) \geqslant 2^k + q - 2.$$

对于 $g(k)$, Виноградов 的方法也能导致非常出色的結果. Dickson[30] 与 Pillai[31] 相互独立地得到了有关 $g(k)$ 問題的几乎最后的解决. 这个解的第一部分也是最深刻的部分,有賴于 Виноградов 方法的应用. 第二部分則依賴于一个称为"上升法"的方法. 它的最后結果是:对于 $k > 6$ 且使

$$\left(\frac{3}{2}\right)^k - \left[\left(\frac{3}{2}\right)^k\right] \leqslant 1 - \left(\frac{1}{2}\right)^k \left\{\left[\left(\frac{3}{2}\right)^k\right] + 3\right\} \tag{106}$$

成立的全体 k,都有

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2. \tag{107}$$

这一条件在 $4 \leqslant k \leqslant 400$ 时成立, 它也可能对全体 $k > 3$ 都成立. 以后, Pillai[31] 証明:对于 $k = 6$, (107)也眞确,亦即 $g(6) = 73$. 于是現在除了 $k = 4$ 及 $k = 5$,以及(106)是否成立尚未获得确定的任何 $k > 3$, 問題的解就完整了. $g(3) = 9$ 很早以前已被 Wieferich 所証得. 对于 $k = 4$ 及 $k = 5$,已知的最佳的不等式是

$$19 \leqslant g(4) \leqslant 35, \quad 37 \leqslant g(5) \leqslant 54;$$

其中的上界都是 Dickson[198] 給出的.

Нечаев[189] 証明了 $g\left(\binom{x}{k}\right) < 6k \log k + 8k \log\log k$.

設 $u = u_i$ 为一形如 x^m 的数,此处 $m \geqslant n$. Pillai[199] 証明:对于全体 $n \geqslant 32$,使方

程 $N = u_1 + \cdots + u_s$ 对于任何 N 都为可解的 s 的最小值都等于

$$2^n + \left[\frac{1}{\log 2} \log \left[\left(\frac{3}{2}\right)^n\right]\right] - 1.$$

29. 齐次問題

用 $N(k)$ 表示使方程組

$$\left.\begin{array}{l} x_1 + \cdots + x_t = y_1 + \cdots + y_t \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^k + \cdots + x_t^k = y_1^k + \cdots + y_t^k \end{array}\right\} \qquad (108)$$

在下述的意义下为可解的最小整数 t: $x_1, \cdots, x_t, y_1, \cdots, y_t$ 都是正整数，但 $y_1, \cdots, y_t$ 不能是 $x_1, \cdots, x_t$ 的重新排列. 又用 $M(k)$ 表示使方程組 (108) 为可解且使

$$x_1^{k+1} + \cdots + x_t^{k+1} \neq y_1^{k+1} + \cdots + y_t^{k+1}$$

成立的最小的 t,显然有

$$k + 1 \leqslant N(k) \leqslant M(k).$$

用初等方法可以証明 $N(k) \leqslant \frac{1}{2} k(k+1) + 1$. Wright[200] 証明了

$$N(k) \leqslant \begin{cases} \frac{1}{2}(k^2 + 3), & \text{假如 } 2 \nmid k, \\ \frac{1}{2}(k^2 + 4), & \text{假如 } 2 \mid k. \end{cases}$$

又华罗庚[201]証明了

$$M(k) \leqslant (k+1)\left(\left[\frac{\log \frac{1}{2}(k+2)}{\log\left(1 + \frac{1}{k}\right)}\right] + 1\right),$$

它是下述的由华罗庚[202]証明的更一般性定理的直接推論.

定理. 設 $j \geqslant (k+1)\left(\left[\frac{\log \frac{1}{2}(k+2)}{\log\left(1 + \frac{1}{k}\right)}\right] + 1\right)$. 对于任何給定的 s, 必存在 $N_1, \cdots, N_k$; $M_1, \cdots, M_s$ (当 $t_1 \neq t_2$ 时, $M_{t_1} \neq M_{t_2}$),使下面 s 組不定方程

$$R_t (1 \leqslant t \leqslant s) \begin{cases} \sum_{i=1}^{j} x_{it}^h = N_h \quad (1 \leqslant h \leqslant k), \\ \sum_{i=1}^{j} x_{it}^{k+1} = M_t \end{cases}$$

都为可解。

华罗庚[26) 82)]还証明了下面的

定理. 設 $k \geqslant 2$，又 t_0 为由下表定义的一个与 k 有关的整数：

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
t_0	3	8	23	55	120	207	336	540	885	$[k^2(3\log k + \log\log k + 4)]$

用 $r_t(P)$ 表示在

$$1 \leqslant x_i,\ y_i \leqslant P$$

的限制下不定方程組(108)的解数，則对 $t > t_0$ 有

$$\lim_{P\to\infty} P^{\frac{1}{2}k(k+1)-2t} r_t(P) = \vartheta_0 \mathfrak{S},$$

此处

$$\vartheta_0 = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \left| \int_0^1 e^{2\pi i(\beta_k x^k + \cdots + \beta_1 x)}\, dx \right|^{2t} d\beta_k \cdots d\beta_1$$

而

$$\mathfrak{S} = \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{\substack{h_1=1\\(h_1,q_1)=1}}^{q_1} \cdots \sum_{\substack{h_k=1\\(h_k,q_k)=1}}^{q_k} \left| q_1^{-1} \cdots q_k^{-1} \sum_{x=1}^{q_1\cdots q_k} e^{2\pi i\left(\frac{h_k}{q_k}x^k + \cdots + \frac{h_1}{q_1}x\right)} \right|^{2t}.$$

定理的証明主要基于 Виноградов 的方法与华罗庚[98)]引进的估計完整指数和的一个新方法。

設 $0 < i < j < \cdots < k$ 为 g 个整数，又 $0 < N_i < N_j < \cdots < N_k$ 为給定的一些整数。命 $N_k = P^k$ (P 是实数)。Марджанишвили[203)]曾經研究过在 N_i 充分大时，不定方程組

$$\left.\begin{aligned} x_1^i + x_2^i + \cdots + x_s^i &= N_i \\ x_1^j + x_2^j + \cdots + x_s^j &= N_j \\ \cdots\cdots&\cdots\cdots \\ x_1^k + x_2^k + \cdots + x_s^k &= N_k \end{aligned}\right\} \tag{109}$$

有否整数解的問題。他証明了下面的

定理. 設 $N_i = h_i P^i$，$N_j = h_j P^j$，$\cdots$，又設 $k \geqslant 12$，$r = [2k\log 10kg + k\log\log 20kg] + 1$，$f > 3kg$ 为給定的常数。如果存在常数 $\varepsilon > 0$，使对 $s = f$，方程組

$$\left.\begin{aligned} \xi_1^i + \xi_2^i + \cdots + \xi_s^i &= h_i \\ \xi_1^j + \xi_2^j + \cdots + \xi_s^j &= h_j \\ \cdots\cdots&\cdots\cdots \\ \xi_1^k + \xi_2^k + \cdots + \xi_s^k &= h_k \end{aligned}\right\}$$

有适合

$$\xi_n \geqslant \varepsilon > 0 \quad (n = 1, 2, \cdots, f)$$

及

$$|\Delta| \geqslant \varepsilon$$

的实数解 $\xi_1, \cdots, \xi_f$,此处

$$\Delta = \begin{vmatrix} \xi_1^{i-1}, & \cdots, & \xi_g^{i-1} \\ \cdots & \cdots & \cdots \\ \xi_1^{k-1}, & \cdots, & \xi_g^{k-1} \end{vmatrix},$$

则对具有 $s = f + 2gr$ 的方程組(109), 它的正整数解 $x_1, \cdots, x_s$ 的解数 $I(N_i, \cdots, N_k; i, \cdots, k; s)$ 适合下面的不等式:

$$I > c(i, \cdots, k; f, g, \varepsilon) N_k^{\frac{f}{k} + 2g\left(1 - \left(1 - \frac{1}{k}\right)^r\right) - \frac{1}{k}(i + \cdots + k)} \mathfrak{S}(N_i, \cdots, N_k; s) + \\ + O\left(N_k^{\frac{f}{k} + 2g\left(1 - \left(1 - \frac{1}{k}\right)^r\right) - \frac{1}{k}(i + \cdots + k) - \frac{\omega}{k}}\right),$$

此处 c 与 ω 为某两个正常数,而 $\mathfrak{S}$ 就是所謂奇异級数.

关于 $\mathfrak{S}$ 为正的性质,已在 Марджанишвили 的工作中探討过.

第五章 Гольдбах 問題

30. Виноградов 定理

用 $r(N)$ 表示将一奇数 N 表成三个素数之和的表法种数，则有

$$r(N)=\int_0^1 (S(\alpha))^3 e^{-2\pi i N\alpha}d\alpha,$$

此处

$$S(\alpha)=\sum_{p\leqslant N} e^{2\pi i\alpha p},$$

p 經过 $\leqslant N$ 的全体素数.

将积分区間移至 $\left(-\frac{1}{\tau},\ 1-\frac{1}{\tau}\right)$，此处 $\tau=NL^{-h}$，而 $L=\log N$，h 为一 $\geqslant 16$ 的正整数. 用 $\mathfrak{M}_{h,q}$ 表示区間

$$\alpha=\frac{a}{q}+\beta,\quad |\beta|\leqslant\frac{1}{\tau},\quad 1\leqslant q\leqslant L^h,\quad (a,q)=1.$$

这些小区間互不重迭. 区間的剩余部分用 E 表示之.

在 $\mathfrak{M}_{h,q}$ 上可有

$$\sum_{p\leqslant N} e^{2\pi i\alpha p}=\sum_{p\leqslant N} e^{2\pi i\left(\frac{a}{q}+\beta\right)p}=$$

$$=\sum_{\substack{r=1\\(r,q)=1}}^{q} e^{2\pi i\frac{ar}{q}}\sum_{n\leqslant N} e^{2\pi i\beta n}(\pi(n;q,r)-\pi(n-1;q,r))+O(q)=$$

$$=\sum_{\substack{r=1\\(r,q)=1}}^{q} e^{2\pi i\frac{ar}{q}}\Bigg(\sum_{n\leqslant N-1}\pi(n;q,r)(e^{2\pi i\beta n}-e^{2\pi i\beta(n+1)})+$$

$$+\pi(N;q,r)e^{2\pi i\beta N}\Bigg)+O(q).$$

由 Siegel-Walfisz 定理(第三章，§ 22，(85))，我們得到

$$\sum_{p\leqslant N} e^{2\pi i\alpha p}=\frac{1}{\varphi(q)}\sum_{\substack{r=1\\(r,q)=1}}^{q} e^{2\pi i\frac{ar}{q}}\Bigg(\sum_{n\leqslant N-1}\operatorname{li} n(e^{2\pi i\beta n}-e^{2\pi i\beta(n+1)})+\operatorname{li} N\cdot e^{2\pi i\beta N}\Bigg)+$$

$$+O(NL^{-4h})=$$

$$=\frac{\mu(q)}{\varphi(q)}\left(\sum_{2<n\leqslant N} e^{2\pi i\beta n}\int_{n-1}^{n}\frac{dt}{\log t}\right)+O(NL^{-4h})=$$

$$=\frac{\mu(q)}{\varphi(q)}\int_2^N\frac{e^{2\pi i\beta t}}{\log t}dt+O(NL^{-4h}),$$

最后一步是因为

$$e^{2\pi i\beta n}-e^{2\pi i\beta t}=2\pi i\beta\int_t^n e^{2\pi i\beta u}du\ll\beta(n-t)\ll\frac{n-t}{\tau}.$$

在 E 上,由第二章 §15 可有

$$|S(\alpha)|\ll NL^{5-\frac{1}{2}h}.$$

所以得到

$$r(N)=\sum_{\mathfrak{M}}\int_{\mathfrak{M}_{a,q}}(S(\alpha))^3e^{-2\pi iN\alpha}d\alpha+O(N^2L^{-4})=$$

$$=\frac{N^2}{2L^3}\mathfrak{S}(N)+O(N^2L^{-4}\log L),\tag{110}$$

式中

$$\mathfrak{S}(N)=\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right).$$

因为

$$\mathfrak{S}(N)>\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)>\prod_{p}\left(1-\frac{1}{p^2}\right)=\frac{6}{\pi^2},$$

故得定理.

附注 1. 除了 Hardy 与 Littlewood 的开創性工作外,我們还要提到 Estermann[204)205)] 的两个結果,这两个結果是在 Виноградов 的重大貢献之前得到的. 他証明了: a)[204)] 每一个大的奇整数都能表成形如 $p_1+p_2+p_3p_4$ 的和数,这里的 p_1, p_2, p_3, p_4 都是素数; b)[205)] 每一个大的整数都是两个素数与一平方数的和.

附注 2. 在 Виноградов 的工作之后, Линник[12) 206)] 与 Чудаков[207)] 給出了另外两个証明,这两証明都以 L-函数在临界带状区域中的零点分布为基础. 更确切地説,所用到的性质是 Dirichlet L-函数 $L(s,\chi)$ 在矩形 $\beta\leqslant\sigma\leqslant 1$, $|t|\leqslant T$ 中的零点个数等于

$$O(q^{2\beta-1}T^{4(1-\beta)(3-2\beta)^{-1}}\log^{10}T+q^{30}),$$

此处 χ 表一 mod q的原特征,又記号 O 中所含的常数与 q 无关.

31. Виноградов 定理的推廣

1) 不少数学工作者研究了有"比例条件"的 Гольдбах 間題,此即

$$N=p_1+p_2+p_3,\quad p_i\sim\frac{1}{3}N$$

在 $N\to\infty$ 时成立. 最好的結果是 Haselgrove[208)] 所宣布的:每一个大的奇整数都能表成

$$N=p_1+p_2+p_3,\quad p_i=\frac{1}{3}N+O(N^{\vartheta})$$

的形状，此处$\frac{63}{64} < \vartheta < 1$.

2）另外一些数学工作者[209) 210) 211) 212)]研究了如下类型的問題：对于$s \geqslant 3$，找出

$$N = a_1 p_1 + a_2 p_2 + \cdots + a_s p_s$$

的可解条件，这里的$a_1, \cdots, a_s$都是給定的整数，而

$$p_\nu \equiv l_\nu \pmod q, \quad 1 \leqslant \nu \leqslant s.$$

对于$s \geqslant 3$，处理这些問題并无本質的困难. 吳方[213)]更进一步推广了这个問題，他在某些条件下建立了

$$\sum_{\nu=1}^{m} a_{\mu\nu} p_\nu = b_\mu \quad (\mu = 1, 2, \cdots, n;\ m \geqslant 2n+1;\ 2 \leqslant p_\nu \leqslant P,\ \nu = 1, 2, \cdots, m)$$

的解数的漸近公式.

32. 关于偶数的 Гольдбах 問題的結果

在 Виноградов 的重要工作之后，很多数学工作者[214—218)]彼此独立地証明了下面的定理：几乎全体偶整数都能表成两个素数之和. 华罗庚的結果較旁人的結果稍強，他証明了$p_1 + p_2^k$表出几乎全体偶数.

Линник 作出了主要的推进.

1)[219)] 在 Riemann 猜測眞确的假定下，对于任何$\varepsilon > 0$及对每一大的整数N，总可以找到两个素数p_1及p_2，使

$$|N - p_1 - p_2| < (\log N)^{3+\varepsilon}$$

成立. 又在一較弱的假定下，也卽如果

$$N(\sigma, T) = O(T^{2(1-\sigma)} \log^2 T),$$

則得

$$|N - p_1 - p_2| < (\log N)^7.$$

由 Ingham 关于相継素数的定理，我們立刻得到$|N-p_1-p_2| < N^{\frac{25}{64}+\varepsilon}$. Линник証明，由此甚至能够得出

$$|N - p_1 - p_2| < N^{0.13}.$$

2)[220)] 对于任何給定的正整数$g > 1$，恆存在正整数k_0，使对任何給定的$k > k_0$，每一个$\equiv kg \pmod 2$的大整数都能用

$$p_1 + p_2 + g^{x_1} + \cdots + g^{x_k}$$

表出，这里的p_1与p_2都是素数，而$x_1, \cdots, x_k$都是正整数.

Rényi[19)] 作出了另一个有趣的推进.

3）存在常数k，使每一大偶数都是某一素数与另一个不超过k个素数的乘积的

和. 在此以前, Бухштаб[221] 証明了:对于任何給定的 $\lambda > 0$, 每一大偶数 N 都能表成 $N = p + N'$ 的形状,这里的 p 是素数,而 N' 的素因子都小于 $(\log N)^\lambda$. 这种表法的个数小于 $cN/(\log N \log\log N)$,而 $c > 0$.

此外, A. Page[157] 証明: 将偶数 N 分解成一个素数与一无平方因子数的方法数等于

$$\prod_p (1-(p^2-p)^{-1}) \prod_{p|N} \frac{p^2-p}{p^2-p-1}\int_2^N \frac{du}{\log u} + O\left(\frac{N}{\log^5 N}(\log\log N)^8 \log\log\log N\right).$$

王元[56] 証明了

4) 在广义 Riemann 猜想眞确的假定下,每一大偶数都是一个素数与一个至多是四个素数乘积的数之和.

Rényi 的証明主要基于 Линник[18] 的所謂"大篩法"的某一改进的应用,就許多关系来説,这个大篩法与 Brun[14] 的方法相似. 这两个方法的主要不同点是:在 Brun 的方法中,由 mod p 的全体剩余类中所除去的类数 k 对一切 p 都是固定的,但在 Линник 的方法中,它們能够随 p 而变. 因为 Линник 的大篩法曾为很多数学工作者[19) 114] 成功地应用过, 所以我們現在把它的輪廓作如下的描述: 設 $p_1, \cdots, p_y$ 为任意 y 个适合 $p_i \leqslant \sqrt{N}$ $(i = 1, \cdots, y)$ 的素数.

定理. 用 $f(p)$ 表一正値函数, $f(p) < p$,又命

$$\tau = \min_{i=1,2,\cdots,y} \frac{f(p_i)}{p_i}.$$

假如从序列 $1, 2, \cdots, N$ 中除去那些属于 mod p_i $(i = 1, \cdots, Y)$ 的 $f(p_i)$ 个确定的剩余类中某一类的整数,则余下的整数个数不超过

$$\frac{20\pi N}{\tau^2 y}.$$

証. 設 $n_1 < n_2 < \cdots < n_Z \leqslant N$ 为从序列 $1, 2, \cdots, N$ 中除去属于 $f(p_i)$ 个 mod p_i $(i = 1, 2, \cdots, y)$ 的剩余类中某一类的那些整数后所余下的整数. 命

$$S(\alpha) = \sum_{j=1}^{Z} e^{2\pi i \alpha n_j},$$

则对 $\delta = \dfrac{\tau}{20\pi N}$,显然有

$$Z = I = \int_0^1 |S(\alpha)|^2 d\alpha \geqslant \sum_{p_j} \sum_{y=1}^{p_j-1} \int_{-\delta}^{+\delta} \left| S\left(\frac{y}{p_j} + x\right)\right|^2 dx = \sum_{p_j} I'_{p_j},$$

这是因为任何两个积分区間都不交迭的原故. 另一方面,我們有

$$I'_p = \sum_{y=0}^{p-1} \int_{-\delta}^{\delta} \left|S\left(\frac{y}{p}+x\right)\right|^2 dx - \int_{-\delta}^{\delta} |S(x)|^2\, dx \geqslant 2\delta p\left(1-\frac{\tau}{10}\right) \sum_{n_i \equiv n_j} \sum_{(\mathrm{mod}\ p)} 1 - 2\delta Z^2.$$

用 a_i 表 $n_1, \cdots, n_Z$ 諸数中与同一 ξ_i 模 p 同余者之个数，则由 Schwarz 不等式，可以得出

$$\sum_{n_i \equiv n_j} \sum_{(\bmod p)} 1 = \left(\sum_i a_i^2\right) \geqslant \frac{\left(\sum_i a_i\right)^2}{p - f(p)} = \frac{Z^2}{p - f(p)} \geqslant \frac{Z^2}{p}(1 + \tau).$$

于是得到

$$Z \geqslant y\delta\tau Z^2 = y\frac{\tau^2}{20\pi N}Z^2.$$

証明完毕.

这个定理具有下述的等价形式:

設 $n_1 < n_2 < \cdots < n_Z \leqslant N$ 为 Z 个正整数. 用 $f(p)$ 表一适合 $f(p) < p$ 的正值函数，而命

$$\tau = \min_{p \leqslant \sqrt{N}} \frac{f(p)}{p} > 0,$$

则至多除了

$$\frac{20\pi N}{\tau^2 Z}$$

个例外的素数外，对于每一素数 $p \leqslant \sqrt{N}$，整数 $n_1, \cdots, n_Z$ 一定分落在不少于 $p - f(p)$ 个不同的模 p 剩余类中.

33. Waring-Гольдбах 問題

§ 33 与 § 35 的結果都可在华罗庚的专著[222]中找到.

1) 設 $I_s(N)$ 是以素数 $p_1, \cdots, p_s$ 为变量的方程

$$p_1^k + \cdots + p_s^k = N$$

的解数，于是对于

$$s \geqslant \begin{cases} 2^k + 1, & \text{当 } 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2.5), & \text{当 } k > 10, \end{cases}$$

可有

$$I_s(N) = \mathfrak{S}(N)\frac{\Gamma^s\left(\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}\frac{N^{\frac{s}{k}-1}}{(\log N)^s} + O\left(\frac{N^{\frac{s}{k}-1}}{(\log N)^{s+1}}\log\log N\right),$$

此处

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} B_s(N, q),$$

$$B_s(N, q) = \sum_{\substack{h=1 \\ (h,q)=1}}^{q} (W_{h,q}/\varphi(q))^s e^{-2\pi i h N/q},$$

$$W_{h,q} = \sum_{\substack{l=1 \\ (l,q)=1}}^{q} e^{2\pi i h l^k/q}.$$

这里所用的原则是找一 t,使

$$\int_0^1 \left| \sum_{x=1}^{P} e^{2\pi i \alpha x^k} \right|^{2t} d\alpha \ll P^{2t-k}$$

成立. 由此并按第二章 § 15 的定理 2,我們得到:对于 $s > 2t$,

$$\int_E \left(\sum_{p \leqslant P} e^{2\pi i \alpha p^k} \right)^s e^{-2\pi i N\alpha} d\alpha \ll (PL^{-\sigma_0})^{s-2t} \int_0^1 \left| \sum_{p \leqslant P} e^{2\pi i \alpha p^k} \right|^{2t} d\alpha \ll$$

$$\ll P^{s-2t} L^{-s_1} \int_0^1 \left| \sum_{x=1}^{P} e^{2\pi i x^k \alpha} \right|^{2t} d\alpha \ll P^{s-k} L^{-s_1},$$

这里的 E 就是所謂"劣弧".

这个結果能够推广到

$$f_1(p_1) + \cdots + f_s(p_s) = N$$

的問題,此处 $f_1, \cdots, f_s$ 为 s 个首項系数为正的整値多項式.

2) 設 $p^\Theta \| k$,而

$$K = \prod_{(p-1)|k} p^\gamma,$$

这里的 γ 当 $p = 2$ 而 $2|k$ 时等于 $\Theta + 2$,在其他情形,則等于 $\Theta + 1$.

用 $H(k)$ 表示具有下述性質的最小整数 s: 它使每一充分大的 $\equiv s \pmod K$ 的整数都能表成 s 个素数的 k 次乘冪之和. 通过研究算术性状,我們便由 1) 得出

$$H(k) \leqslant \begin{cases} 2^k + 1, & \text{当 } 1 \leqslant k \leqslant 10, \\ 2k^2(2\log k + \log\log k + 2.5), & \text{当 } k > 10. \end{cases}$$

因此, 每一大奇数都是三个素数的和; 每一个 $\equiv 5 \pmod{24}$ 的大整数都是五个素数的平方之和;每一大奇数都是九个素数的立方之和.

更进一步,我們有

$$H(k) \leqslant 2k + 2m + 7,$$

此处

$$m = \left[\frac{\log \frac{1}{2} b + \log\left(1 - \frac{2}{k}\right)}{-\log\left(1 - \frac{1}{k}\right)} \right], \quad b = \begin{cases} 2k^2(2\log k + \log\log k + 3), & \text{当 } k > 12, \\ 2^{k-1}, & \text{当 } k \leqslant 12. \end{cases}$$

讀者注意, $2k + 2m + 7 \sim 4k \log k$.

借助于 Davenport 的引理,我們还能得到

$$H(4) \leqslant 15,\quad H(5) \leqslant 25,\quad H(6) \leqslant 37,\quad H(7) \leqslant 55,\quad H(8) \leqslant 75.$$

34. 問題的变形

Halberstam[223] 証明:几乎全体正整数 m 都能表成 $p_1^2 + p_2^3 + x^3$ 的形状,这里的 p_1, p_2 都是素数,而 x 为一正整数.

Prachar[224] 証明:几乎全体偶整数都能表成

$$p_1^2 + p_2^3 + p_3^4 + p_4^5$$

的形状,这里的 p_1, p_2, p_3, p_4 都是素数;他还証明了,全体充分大的奇数都能表成

$$p_1 + p_2^2 + p_3^3 + p_4^4 + p_5^5$$

的形状.

設 $c > 1$ 非整数, И. И. Шапиро-Пятецкий[225] 証明:对于任何給定的 $\varepsilon > 0$, 存在 $N_0 = N_0(\varepsilon)$,使对任何实数 $N > N_0$,当 $r \geqslant H(c)$ 时,不等式

$$|p_1^c + \cdots + p_r^c - N| < \varepsilon$$

都有素数解. 他还証明了

$$\varlimsup_{c\to\infty} \frac{H(c)}{c \log c} \leqslant 4.$$

35. 齐次問題(請参考 Марджанишвили[226])

1) 对于任何整数 $k \geqslant 2$,用 $I(N_1, \cdots, N_k)$ 表示满足方程組

$$p_1^k + \cdots + p_s^k = N_k,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$p_1 + \cdots + p_s = N_1$$

的素数組 $p_1, \cdots, p_s$ 的組数.

設 s_0 为由下表給出的数值:

k	2	3	4	5	6	7	8	9	10	$\geqslant 11$
s_0	7	19	49	113	243	417	675	1083	1773	$2k^2(3\log k + \log\log k + 4)$

并置 $[N_k^{\frac{1}{k}}] = P$,则对 $s \geqslant s_0$,渐近公式

$$I(N_k, \cdots, N_1) = b_1 P^{s-\frac{1}{2}k(k+1)} L^{-s} \mathfrak{S}(N_k, \cdots, N_1) + O(P^{s-\frac{1}{2}k(k+1)} L^{-s-1} \log L)$$

成立,此处

$$b_1 = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \left(\int_0^1 e^{2\pi i(\gamma_k x^k + \cdots + \gamma_1 x)} dx\right)^s e^{-2\pi i(N_k P^{-k} \gamma_k + \cdots + N_1 P^{-1} \gamma_1)} d\gamma_k \cdots d\gamma_1,$$

$$\mathfrak{S}(N_k, \cdots, N_1) = \sum_{q_1, \cdots, q_k=1}^{\infty} A(q_k, \cdots, q_1),$$

$$A(q_k, \cdots, q_1) = \sum_{h_1, \cdots, h_k}{}' T^s e^{-2\pi i\left(\frac{h_k N_k}{q_k}+\cdots+\frac{h_1 N_1}{q_1}\right)},$$

$$T = \frac{1}{\varphi(Q)} \sum_{x}{}' e^{2\pi i\left(h_k \frac{x^k}{q_k}+\cdots+h_1 \frac{x}{q_1}\right)},$$

Q 是 $q_1, \cdots, q_k$ 的最小公倍数，$h_1, \cdots, h_k$ 分别通过 mod $q_1, \cdots,$ mod q_k 的縮剩余系，而 x 则通过 mod Q 的縮剩余系.

2）我們也得到了保証主項确实大于誤差項的两个条件，它們是 1)“阶条件”与 2)“同余条件”. 实际上，1) 保証了方程組：

$$x_1^h + \cdots + x_s^h = N_h, 1 \leqslant h \leqslant k$$

具有正解，而2)保証了同余組：

$$x_1^h + \cdots + x_s^h \equiv N_h \pmod q, \quad 1 \leqslant h \leqslant k$$

对于全体 $q \geqslant 1$ 都可解.

更多的結果可在 § 33 开始时所引到的华罗庚的专著[23] 中找到.

第六章　一致分布

36. 定义与 Weyl 判别法则

設 $f(x)$ 为一实函数. 对于給定的滿足 $0 \leqslant a \leqslant b \leqslant 1$ 的 a 与 b,用 $N(P; a, b)$ 表示使

$$a \leqslant \{f(n)\} < b \tag{111}$$

成立的整数 $n \leqslant P$ 的个数,这里的 $\{f(n)\}$ 表示 $f(n)$ 的分数部分. 如果

$$\lim_{P\to\infty} \frac{N(P; a, b)}{P} = b - a, \tag{112}$$

則称 $f(x)$ 模 1 一致分布.

Weyl[20] 給出了下面的重要判別法則.

定理 1. 如果 $f(x)$ 模 1 一致分布,則对任何黎曼可积函数 $w(t)$,都有

$$\lim_{P\to\infty} \frac{1}{P} \sum_{x=1}^{P} w(\{f(x)\}) = \int_0^1 w(t)dt. \tag{113}$$

这几乎可以从黎曼积分的定义立刻导出. 又取 $w(t) = 1$ (当 $a \leqslant x < b$ 时), $w(t) = 0$ (在其他点上),就立刻得到逆定理.

在黎曼可积函数的集合中,我們选出一个特殊序列

$$e^{2\pi iht}, \quad h = 0, \pm 1, \pm 2, \cdots. \tag{114}$$

(114)的綫性包給出每一黎曼可积函数,这就建議了

定理 2 (Weyl 判別法則). 当且仅当

$$\lim_{P\to\infty} \frac{1}{P} \sum_{x=1}^{P} e^{2\pi ihf(x)} = 0$$

对于任何确定的整数 $h \neq 0$ 都成立时,函数 $f(x)$ 模 1 一致分布.

証. 充分性的証明. 設 $G(t)$ 为一具有周期 1 的函数,当 $0 \leqslant t < \gamma$ 时, $G(t) = 1$;当 $\gamma \leqslant t < 1$ 时, $G(t) = 0$. 于是

$$N(P; 0, \gamma) = \sum_{x=1}^{P} G(f(x)).$$

命 η 为一适合不等式 $2\eta < \gamma$ 与 $2\eta < 1 - \gamma$ 的正数. 我們作出两个輔助函数 $G_1(t)$ 与 $G_2(t)$,它們都有周期 1,并且适合

$$G_2(t) \leqslant G(t) < G_1(t).$$

又 $G_1(t)=1$ (当 $0\leqslant t\leqslant\gamma$), $=0$ (当 $\gamma+\eta\leqslant t\leqslant 1-\eta$), 而在 $-\eta\leqslant t\leqslant 0$ 与 $\gamma\leqslant t\leqslant\gamma+\eta$ 中它为綫性函数; $G_2(t)=1$ (当 $\eta\leqslant t\leqslant\gamma-\eta$), $=0$ (当 $\gamma\leqslant t\leqslant$ $\leqslant 1$),在 $0\leqslant t\leqslant\eta$ 与 $\gamma-\eta\leqslant t\leqslant\gamma$ 中也为綫性函数. 因为 G_1, G_2 都为連續,故有一致收斂的富里埃級数展开:

$$G_1(t)=\gamma+\eta+\sum_{h=1}^{\infty}(a_he^{2\pi iht}+b_he^{-2\pi iht}),$$

$$G_2(t)=\gamma-\eta+\sum_{h=1}^{\infty}(a'_he^{2\pi iht}+b'_he^{-2\pi iht}).$$

在这两級数中,都置 $t=f(x)$,并对 $x=1, 2, \cdots, P$ 相加,就得到

$$\lim_{P\to\infty}\frac{N(P;0,\gamma)}{P}=\gamma.$$

我們先研究綫性的情形. 因为对于任何整数 $h\neq 0$ 与对任何无理数 α,都有

$$\lim_{P\to\infty}\frac{1}{P}\left|\sum_{x=1}^{P}e^{2\pi ih\alpha x}\right|\leqslant\lim_{P\to\infty}\min\left(1,\ \frac{1}{|\sin\pi h\alpha|P}\right)=0.$$

故得

定理 3. 对于任何实无理数 α,序列

$$\alpha,\ 2\alpha,\ 3\alpha,\ \cdots$$

模 1 一致分布.

由定理 2 我們能够导出

定理 4. 設 $f(x)$ 为一非常数的并且至少有一无理系数的多項式,则序列

$$f(x),\quad x=1,\ 2,\ \cdots$$

模 1 一致分布.

Van der Corput[227] 将此概念加以推广,从而得到了

定理 5. 如果对于任何固定的正整数 q, $f(x+q)-f(x)$ 模 1 一致分布,则函数 $f(x)$ 模 1 一致分布.

Weyl 也証明了

定理 6. 設 $g(x)$ $(x=1, 2, 3, \cdots)$ 为一列互不相同的整数,则对几乎全体 α,函数 $\alpha g(x)$ 模 1 一致分布(这里的"几乎全体"是按勒貝格意义而言).

为了証明这个定理,我們利用恆等式

$$\int_0^1\left|\frac{1}{N}\sum_{x=1}^{N}e^{2\pi ih\alpha g(x)}\right|^2 d\alpha=\frac{1}{N},\quad \alpha\neq 0,\quad h\ \text{是非 0 整数}.$$

由此我們能够估計那些使被积函数大于一个給定正数的 α 所成集合测度的上界.

另一方面,对于任何給定的实数 α,我們能够容易地构造出一列整数 $g(x)$ $(x=$

$=1, 2, \cdots$),使 $\alpha g(x)$ ($x=1, 2, \cdots$) 模 1 并不一致分布。

Koksma[228] 用 Weyl 的方法証明了

定理 7. 对于几乎全体实数 $\alpha \geqslant 1$, 序列 α^x($x=1, 2, \cdots$) 都模 1 一致分布。

但到現在为止,人們还不知道 e^x 是否模 1 一致分布。

37. 誤差項的估計

采用 § 36 中的記号,我們称函数

$$R(P) = N(P; a, b) - (b-a)P \tag{115}$$

为誤差項,而称

$$D(P) = R(P)/P \tag{116}$$

为离差。如果 $f(x)$ 模 1 一致分布,則

$$R(P) = o(P). \tag{117}$$

根据第二章 § 7 的結果,我們有下面的

定理 1 (Виноградов[229]). 設 $k \geqslant 2$, $P \geqslant 1$,又設

$$f(x) = \alpha x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k,$$

$$\left|\alpha - \frac{h}{q}\right| < \frac{1}{q^2}, \quad (h, q) = 1, \quad 1 \leqslant q \leqslant P^k,$$

則对 $f(x)$ 的离差 $D(P)$,我們得到:对于任何 $\varepsilon > 0$,

$$D(P) = O(L), \quad L = P^\varepsilon(P^{-1} + q^{-1} + qP^{-k})^{2^{1-k}}$$

成立。

为了証明这个定理,取 $\eta = P^{-2^{1-k}} < \frac{1}{3}$ 及

$$0 < \gamma < 1 - 2\eta,$$

并如 § 36 中那样定义 $G_1(t)$ 与 $G_2(t)$,于是不难得到

$$|a_h| \leqslant \min\left(\frac{1}{h}, \frac{1}{\eta h^2}\right), \quad |b_h| \leqslant \min\left(\frac{1}{h}, \frac{1}{\eta h^2}\right).$$

由此

$$N(P; 0, \gamma) = \sum_{x=1}^{P} G(f(x)) \leqslant \sum_{x=1}^{P} G_1(f(x)) =$$

$$= (\gamma + \eta)P + 2\sum_{h=1}^{P} \frac{1}{h}\left|\sum_{x=1}^{P} e^{2\pi i h f(x)}\right| + O(P^{1-2^{1-k}}).$$

証明的主要部分在于二重指数和的估計,而由第二章 § 7 知道它 $\ll PL$,因此

$$N(P; 0, \gamma) \leqslant \gamma P + O(PL).$$

类似地，我們用 $G_2(x)$ 代替 $G_1(x)$，便得

$$N(P;0,\gamma)\geqslant \gamma P+O(PL).$$

所以

$$R(P)=O(PL).$$

如用 Виноградов 更精密的結果，我們能够得出

定理 2. 設 $k\geqslant 11$，

$$f(x)=a_{k+1}x^{k+1}+\cdots+a_1x$$

为一实系数多項式；又設 s 为 $k+1,\cdots,2$ 諸数之一，并且

$$\left|a_s-\frac{h}{q}\right|<\frac{1}{q^2},\quad (h,q)=1,\quad q>0,$$

則有

$$R(P)=O(P^{1-\rho}),$$

此处

$$\rho=\tau/3k^2\log\frac{12k(k+1)}{\tau},$$

τ 随 P 与 q 而变，它的定义如下：

$$\begin{aligned} q&=c_1P^{\tau}, && \text{当 } 1<q\leqslant c_1P,\\ \tau&=1, && \text{当 } c_1P\leqslant q\leqslant c_2P^{s-1},\\ q&=c_2P^{s-\tau}, && \text{当 } c_2P^{s-1}\leqslant q\leqslant c_3P^{s}, \end{aligned}$$

c_1, c_2, c_3 都是确定的正常数.

对于 $2\leqslant k\leqslant 10$，用 Weyl 的估計（第二章 § 7），我們得到一个类似的結果. 对于綫性与二次多項式 $f(x)$，大量的更进一步的結果已为很多数学工作者所获得（参見 Koksma[230]）.

更一般地，Erdös 与 Turán[231] 証明了：如果 $\varphi_1,\cdots,\varphi_P$ 都是实的，又若对全体正整数

$$k\leqslant m=m(P),$$

不等式

$$\left|\sum_{\nu=1}^{P}e^{2\pi ik\varphi_\nu}\right|\leqslant\psi(k)$$

成立，則

$$R(P)=O\left(\frac{P}{m+1}+\sum_{k=1}^{m}\frac{\psi(k)}{k}\right).$$

它是 Koksma[230] 一个定理的改进.

附注. 如果 $\{f(1)\}, \{f(2)\}, \cdots$ 构成一无穷序列,則有

$$\varlimsup_{P\to\infty} \bar{R}(P)\frac{\log\log\log P}{\log\log P} \geqslant \frac{1}{2},$$

此处

$$\bar{R}(P) = \varlimsup_{0\leqslant a<b\leqslant 1} |N(P; a, b) - (b-a)P|.$$

因此,不可能有实函数 $f(x)$,使它对 $x = 1, 2, \cdots$ 有无穷多个不相同的分数部分,且有有界的誤差項. 这个結果属于 van Aardenne-Ehrenfest[232],它回答了 van der Corput 提出的一个問題.

38. 以素数为变数的函数的分布

一旦 Виноградов 証明了他的著名的"三素数"定理,他的方法实际上也包含了关于函数 αp 的模 1 一致分布問題的解决,这里的 p 跑过全体素数. 事实上,由 Weyl 判别法則可知,充分而又必要的是去証明:对于任何固定的整数 $h \neq 0$,

$$\sum_{p\leqslant P} e^{2\pi i \alpha h p} = o(\pi(P)), \quad \alpha \text{ 是一无理数}. \tag{118}$$

命 $\tau = P(\log P)^{-\sigma}$ $(\sigma \geqslant 16)$, 又命 $\frac{p_n}{q_n}$ 为 αh 的第 n 个漸近分数; 对于任何給定的 $\varepsilon > 0$, 取 q_{n_0} 很大, 使对任何整数 $q > \frac{q_{n_0}}{2}$,恆有

$$\varphi(q) > \frac{1}{\varepsilon}.$$

又取 P_0 很大,使 $\tau_0 = P_0(\log P_0)^{-\sigma} > q_{n_0}$,則对任何 $P > P_0$, 恆存在一 $n \geqslant n_0$, 使不等式

$$q_n \leqslant \tau < q_{n+1}$$

成立. 于是

$$\left| h\alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n \tau}.$$

如果 $q_n \leqslant \log^\sigma P$,則由 Siegel-Walfisz 定理(第三章, § 22, (85)),我們得到

$$\sum_{p\leqslant P} e^{2\pi i h\alpha p} = \frac{\mu(q_n)}{\varphi(q_n)} \int_2^P \frac{e^{2\pi i\left(h\alpha - \frac{p_n}{q_n}\right)t}}{\log t}\, dt + O(Pe^{-c\sqrt{\log P}}).$$

由此导出(118). 如果 $\log^\sigma P < q_n < P(\log P)^{-\sigma}$, 則用 Виноградов 定理(第二章, § 15),

$$\sum_{p\leqslant P} e^{2\pi i h\alpha p} = O(P(\log P)^{-3}),$$

也得到(118).

Виноградов 对大多数有兴趣的情形获得了更好的誤差項. 他用到下面的估計:

定理 1. 假設 τ 满足不等式

$$P^{\frac{1}{2}} \leqslant \tau \leqslant P e^{-(\log P)^{\varepsilon_0}},$$

又設

$$\left| \alpha - \frac{h}{q} \right| \leqslant \frac{1}{q\tau}, \quad (h, q) = 1$$

及 $e^{(\log P)^{\varepsilon_0}} \leqslant q \leqslant \tau$, 幷命 $\Delta = (q^{-1} + qP^{-1})^{\frac{1}{2}}$,

$$S = \sum_{m=1}^{K} \left| \sum_{p \leqslant P} e^{2\pi i m p \alpha} \right|,$$

而 $K \ll \Delta^{-2}$, 則有

$$S \ll KP(\Delta^{1-\varepsilon} + P^{-\frac{1}{3}+\varepsilon}).$$

用此定理及 § 37 的方法,我們得到

定理 2. 在与定理 1 相同的假定下,用 $H(P)$ 表示适合

$$\{\alpha p\} \leqslant \beta, \quad p \leqslant P$$

的素数 p 的个数,此处 $0 < \beta < 1$, 則有

$$H(P) = \beta\pi(P) + O(P\gamma),$$

而

$$\gamma = (q^{-1} + qP^{-1})^{\frac{1}{2}-\varepsilon} + P^{-\frac{1}{3}+\varepsilon}.$$

特别,如果 α 为一具有有界部分商的无理数,則能这样选取 q, 使它落在 $\sqrt{P}$ 的两个常数倍的中間. 于是得到

$$H(P) = \beta\pi(P) + O(P^{\frac{4}{5}+\varepsilon}),$$

这里的誤差項异常地好. 与作为 P 的函数的 $\pi(P)$ 相比, 它比后者的漸近表示中任何已得的誤差項要优越得多.

設 $f(x)$ 为一多項式,它的首項系数是无理数,則 $\{f(p)\}$ 模 1 一致分布[233]. 对于无理数 α, $\{\alpha p\}$ 为模 1 一致分布的結果, 先是由 Turán[234] 在广义 Riemann 假設下証得的.

39. $\{a^x\}$ 的分布

在 § 36 中, 我們已經看到,对于几乎全体实数 a, $\{a^x\}$ 都是一致分布的. 但对某一給定的 a, $\{a^x\}$ 是否一致分布的問題, 至今还未获得解决. 特别, 我們还不知道 $\{e^x\}$ 是否一致分布.

Постников[235] 用 Виноградов 方法証明了下面的判别法则.

定理 1. 設 q 为一 $\geqslant 2$ 的整数, α 为一实数,用 $N(P; a, b)$ 表示使 $a \leqslant \{\alpha q^x\} \leqslant b$ $(0 \leqslant a < b \leqslant 1)$ 的整数 $x \leqslant P$ 的个数. 如果存在常数 $c > 1$ 及 $k > 0$,使

$$\overline{\lim_{P\to\infty}} \frac{N(P; a, b)}{P} \leqslant c(b-a)\left(1+\log\frac{1}{b-a}\right)^k$$

对任何 a 与 b 都成立,则函数 αq^x 模 1 一致分布.

Коробов[236] 得到了下面的結果.

定理 2. 設 $q \geqslant 2$ 为一固定的整数,

$$\rho_n(q) = \delta_1 \cdots \delta_{q^n+n-1}, \quad 0 \leqslant \delta_i \leqslant q-1, \quad 1 \leqslant i \leqslant q^n+n-1,$$

此处 $\delta_1\delta_2\cdots\delta_n$, $\delta_2\delta_3\cdots\delta_{n+1}$, $\cdots$, $\delta_{q^n}\delta_{q^n+1}\cdots\delta_{q^n+n-1}$ 等 q^n 个数互不相同;又命

$$\rho'_n(q) = \delta_1 \cdots \delta_{q^n},$$

而 $\psi(\mu)$ 为适合 $\lim\limits_{\mu\to\infty} \psi(\mu) = \infty$ 的任何正整值函数;最后,命

$$\alpha = 0 \cdot \underbrace{\rho'_1(q) \ \cdots \ \rho'_1(q)}_{\psi(1)} \ \underbrace{\rho'_2(q) \ \cdots \ \rho'_2(q)}_{\psi(2)} \cdots \underbrace{\rho'_\mu(q) \cdots \rho'_\mu(q)}_{\psi(\mu)} \cdots,$$

则 $\{\alpha q^x\}$ 一致分布.

定理 3. 設 $\varphi(x)$ 为一实値函数,对于任意給定的不全为零的整数 $m_1, \cdots, m_s$,假設和数

$$m_1\varphi(x+1) + \cdots + m_s\varphi(x+s), \quad (x = 1, 2, \cdots)$$

模 1 一致分布,又命

$$\beta = \sum_{k=1}^{\infty} [\{\varphi(k)\}q]/q^k,$$

则 $\{\beta q^x\}$ 一致分布.

Коробов[237] 还証明了:如果 $\lambda > 1$ 为一代数整数,并且适合某种条件,则 $\{\alpha\lambda^x\}$ 一致分布,此处

$$\alpha = \sum_{i=1}^{\infty} \frac{\varphi(i)\gamma_i}{p_i(\lambda^{\tau_i}-1)}\left(\frac{1}{\lambda^{n_i}} - \frac{1}{\lambda^{n_{i+1}}}\right).$$

式中的 p_i, n_i, τ_i, $\varphi(i)$ 都是整数, γ_i 为一有理数, 它們每一个都受到某些条件的限制.

40. 不定不等式

設 $f(x)$ 模 1 一致分布,它有离差 $D(P)$,亦即,适合

$$\gamma - \varepsilon \leqslant \{f(x)\} \leqslant \gamma + \varepsilon$$

的整数 $x \leqslant P$ 的个数等于 $2\varepsilon P + PD(P)$. 于是对于 $\varepsilon > \frac{1}{2}|D(P)|$,存在整数 x,使

$$|\{f(x)\} - \gamma| < \varepsilon \tag{119}$$

成立. 特别,如設 $k \geqslant 11$ 及

$$f(x) = \alpha_{k+1}x^{k+1} + \cdots + \alpha_1 x, \quad \left|\alpha_s - \frac{h}{q}\right| < \frac{1}{q^2},$$

则由 § 37 定理 2,我們得出:存在整数 $x \leqslant P$,使对大的 P,

$$|\{f(x)\} - \gamma| \ll P^{-\rho}$$

成立. Виноградов 推广了这个定理.

定理. 設

$$f(x) = \alpha_h x^h + \cdots + \alpha_k x^k$$

为一实系数多項式,此处 $h < \cdots < k$ 都是正整数. 又設 α_l 为 x^l 的系数,并且

$$\left|\alpha_l - \frac{a}{q}\right| < \frac{1}{q^2}, \quad (a, q) = 1.$$

用 g 表示 $f(x)$ 的非零系数的个数,而 D 表它們的足标的和,则必存在一个具有下之性质的 $c_0(k)$:对于 $q > c_0(k)$,存在整数 x,使

$$|\{f(x)\} - \gamma| < q^{-\rho}, \quad 0 < x < q^{\frac{2}{l}}$$

成立,此处

$$\rho = \frac{\log D}{4kgl(\log D + 1)\log(D\log D + D)}.$$

第七章　其他数論函数

41. 引　言

如果 $f(n)$ 对正整数 n 有定义，则称它为一数論函数．如果对 $(m, m')=1$，有 $f(m)f(m')=f(mm')$，则称它为积性的．又如 $f(m)f(m')=f(mm')$ 常成立，则称它为完全积性的．

下列数論函数在文献中經常出現．

a）Möbius 函数 $\mu(n)$ 与其絕对値 $|\mu(n)|$ 都是积性的．

b）Euler 函数 $\varphi(n)$，它表示 $\leqslant n$ 且与 n 互素的正整数个数．

c）除数函数 $d(n)$，它表示 n 的正因子个数，或更一般的有

$$\sigma_a(n)=\sum_{d\mid n} d^a.$$

d）函数 $r(n)$，它表示将整数 n 分解成两个平方之和的方法数，或更一般的有

$$r_m(n)=\sum_{n_1^2+\cdots+n_m^2=n} 1.$$

可以举出大量的数論函数，但在这里，我們只准备給出其中极少数几个能与数論的解析方法紧密結合的数論函数的結果．

有关数論函数 $f(n)$ 的問題，主要是关于 $f(n)$ 的性状与对大的 n，$f(n)$ 的均值性状的問題．

对于前一种情形，我們討論下述各种問題：設法找一函数 $\psi(n)$，使 $|f(n)|<\psi(n)$ 对全体 n，对几乎全体 n，或对无穷多个 n 成立．对于函数 $\frac{1}{f(n)}$，也有类似的問題，它也是一数論函数．

例如，我們有 $\varphi(n)\leqslant n-1$ 及

$$e^{-\gamma}=\varliminf_{n\to\infty}\frac{\varphi(n)\log\log n}{n}.$$

又有

$$2\leqslant d(n),$$

$$\varlimsup_{n\to\infty}\frac{\log d(n)\log\log n}{\log n}=\log 2,$$

$$\varlimsup_{n\to\infty}\frac{\sigma(n)}{n\log\log n}=e^{\gamma},$$

此处 γ 表 Euler 常数.

第二种情形，也就是关于平均值的問題，在解析数論中占有更重要的地位. 通常,我們能够給出一个漸近公式

$$\sum_{n\leqslant N} f(n) = P(N) + R(N),$$

$\dfrac{R(N)}{P(N)}$ 于 $N\to\infty$ 时趋向于 0. 主要問題在于寻求 $R(N)$ 的最优阶. 还有另外一些問題,如关于 $R(N)$ 的 Ω-結果与 $R(N)$ 的平均阶的問題等.

对于数論函数 $f(n)$，我們定义

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \quad s = \sigma + it$$

为它的生成函数. 通常,它在某一右半平面如 $\Re s > \sigma_0$ 中正則. 大家知道

$$\sum_{n\leqslant x} f(n) = \frac{1}{2\pi i}\int_{\sigma_1-i\infty}^{\sigma_1+i\infty} F(s)\,\frac{x^s}{s}\,ds \quad (\sigma_1 > \sigma_0).$$

常用的办法是将积分途径移到 $\sigma = -\infty$，而得到一个与 Riemann - von Mangoldt 素数公式类似的显式,或者将它移到某一直綫[233],而得到一个附有誤差項的漸近公式.

42. $\sum_{n\leqslant x}\sigma_a(n)$ 与 $\sum_{n\leqslant x} r_m(n)$ 的表示式

命

$$F(z) = \sum_{n=1}^{\infty} a_n \lambda_n^{-2z-k},$$

$\{a_n\}$ 与 $\{\lambda_n\}$ 为两个給定的序列. 为了这里的目的,我們假定 $a_n = O(n^\varepsilon)$ 及

$$n^{\frac{1}{2}} \ll \lambda_n \ll n^{\frac{1}{2}}.$$

于是从著名的公式

$$\pi i e^{\frac{1}{2}k\pi i} H_k^{(1)}(2is) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} s^{-2z}\Gamma\left(z-\frac{k}{2}\right)\Gamma\left(z+\frac{k}{2}\right)dz,$$

其中 $H_k^{(1)}(s)$ 为第一类 Hankel 函数,我們能够得到

$$f_k(s) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} s^{-2z}F(z)\Gamma\left(z-\frac{k}{2}\right)\Gamma\left(z+\frac{k}{2}\right)dz =$$

$$= \pi i e^{\frac{1}{2}k\pi i}\sum_{n=1}^{\infty} a_n\lambda_n^{-k} H_k^{(1)}(2i\lambda_n s).$$

另一方面,如将积分途径移到 $\sigma = -a$，这里的 a 适合不等式

$$\frac{1}{2}k < a < \min\left(\frac{1}{2}k+1,\ 2\left[\frac{1}{2}+\frac{k}{2}\right]+1-\frac{k}{2}\right),$$

则得

$$f_k(s) = \varphi_k(s) + \frac{1}{2\pi i}\int_{-a-i\infty}^{-a+i\infty} s^{-2z} F(z)\Gamma\left(z - \frac{k}{2}\right)\Gamma\left(z + \frac{k}{2}\right) dz,$$

此处 $\varphi_k(s)$ 为求积函数在带状区域 $-a < x < c$ 中的各个留数之和. 故若 $F(z)$ 在直綫 $\sigma = -a$ 上的性状为已知，则由此我們能够导得 $f_k(s)$ 的另一公式. 将这两公式代入积分

$$\frac{1}{2\pi i}\int_{c-i\tau'}^{c+i\tau'} f_k(s) I_{1+k}(4\pi i s\sqrt{x})\left(1 - \frac{s^4}{\tau^4}\right)^\lambda ds,$$

而取适当的 λ, τ', τ, 我們便能得到 $\sum\limits_{n\leqslant x} a_n$ 的一个表示式. 当 $a_n = \sigma_a(n)$ 时，我們取 $F(s) = \zeta\left(s - \frac{a}{2}\right)\left(s + \frac{a}{2}\right)$, $\lambda_n = 4\pi\sqrt{n}$; 而对 $a_n = r_m(n)$, 则取

$$k = \frac{m}{2} - 1, \quad \lambda_n = 2\pi\sqrt{n}, \quad F(s) = \zeta_m\left(s + \frac{k}{2}\right),$$

此处 $\zeta_m(s)$ 为在 $\sigma > \frac{m}{2}$ 时由等式

$$\zeta_m(s) = \sum{}' \frac{1}{(n_1^2 + \cdots + n_m^2)^s}.$$

表示的 Epstein ζ-函数.

Oppenheim[239] 證明了

$$\sum_{n\leqslant x}\sigma_a(n) - \frac{1}{2}\sigma_a(x) = \Phi_a(x) - x^{\frac{1}{2}+\frac{a}{2}}\sum_{n=1}^{\infty}\frac{\sigma_a(n)}{n^{\frac{1}{2}+\frac{a}{2}}}\left\{\sin\frac{1}{2}a\pi I_{1+a}(4\pi\sqrt{nx}) + \right.$$

$$\left. + \cos\frac{1}{2}a\pi\left[Y_{1+a}(4\pi\sqrt{nx}) + \frac{2}{\pi}K_{1+a}(4\pi\sqrt{nx})\right]\right\}, \qquad (120)$$

这里的 $\Phi_a(x)$ 为 $z^{-1}\zeta(z)\zeta(z-a)x^z$ 的各个留数之和; 級数在 $|a| \geqslant \frac{1}{2}$ 时对于任何 $\varepsilon > 0$ 都 $\left(R, n, |a| - \frac{1}{2} + \varepsilon\right)$ 可和, 而在 $|a| < \frac{1}{2}$ 时收斂. 又

$$\sum_{n\leqslant x} r_m(n) - \frac{1}{2}r_m(x) = \frac{\pi^{\frac{m}{2}}}{\Gamma\left(1 + \frac{m}{2}\right)}x^{\frac{m}{2}} + x^{\frac{m}{2}}\sum_{n=1}^{\infty}\frac{r_m(n)}{n^{\frac{1}{4}m}} I_{\frac{1}{2}m}(2\pi\sqrt{nx}),$$

这里的級数在 $m = 2$ 时收斂, 而在 $m > 2$ 时 $\left(R, n, \frac{1}{2}(m-3) + \varepsilon\right)$ 可和.

在这两情形中，可和性与收斂性在任何不包含 x 的整数值的閉区間中都是一致的.

对于具有行列式 D 的任何正定二次型 $Q(x_1, \cdots, x_m) = \sum a_{ij}x_i x_j$, 也有类似的

結果．亦卽，如用 $r_m(n)$ 表示 $Q=n$ 的解数，則相应地可以得到

$$\sum_{n\leqslant x} r_m(n)-\frac{1}{2} r_m(x)=\frac{\pi^{\frac{m}{2}} x^{\frac{m}{2}}}{\sqrt{D}\, \Gamma\left(\frac{m}{2}+1\right)}-1+\frac{1}{\sqrt{D}} x^{\frac{m}{4}} \sum_{n=1}^{\infty} \frac{r_m(n)}{n^{\frac{m}{4}}} I_{\frac{1}{2}m}(2\pi\sqrt{nx}).$$

43. 一般区域中的整点問題

Виноградов 与 van der Corput 互相独立地发展了处理一般区域中的整点問題的方法，他們的方法也包含了 Voronoi 与 Sierpinski 的結果．Виноградов 的方法比較早些，也比較簡单些(就其在"数論基础"[68]一书中的最后叙述形式而言)，但由它所得的結果要比用 van der Corput 方法得到的差一对数因子（这对圓内整点問題与除数問題都不生影响）．另一方面，Jarník 指出，van der Corput 定理是它这类定理中的最优的．Van der Corput 的結果叙述如下：

設函数 $f(u)$ 在区間 $\frac{1}{2}\leqslant u\leqslant w$ 中具有二阶連續导数，并且 $f\left(\frac{1}{2}\right)>2$，$0<$ $<f'(u)<1$，$f''(u)>z^{-3}$，$z>1$．用 $\mathfrak{G}$ 表示区域 $\frac{1}{2}\leqslant u\leqslant w$，$\frac{1}{2}\leqslant v\leqslant f(u)$．設 $I(\mathfrak{G})$ 为 $\mathfrak{G}$ 的面积，而 $A(\mathfrak{G})$ 为 $\mathfrak{G}$ 中所含的整点个数，則有

$$|A(\mathfrak{G})-I(\mathfrak{G})|\ll z^2. \tag{121}$$

Jarník 构造出了一个适合前述条件的函数，而在曲綫

$$v=f(u),\quad \frac{1}{2}\leqslant u\leqslant w$$

上有多于 cz^2 个整点．

44. 圓内整点問題与除数問題

用 $r(n)$ 表示将非負整数 n 分解成两个平方之和的分法种数．和数 $A(x)=$ $=\sum_{0\leqslant n\leqslant x} r(n)$ 就等于落在圓 $u^2+v^2\leqslant x$ 中的整点 (u,v) 的个数．Gauss[66] 首先証明了

$$A(x)=\pi x+O(\sqrt{x}). \tag{122}$$

以后，Jarník[240] 推广了他的証明原則，而証明了下面的一般結果：設 D 为一封閉的有长 Jordan 曲綫，L 为它的长，A 为它所围的面积，而 N 为含在 D 内的整点个数，則有

$$|A-N|<L.$$

現在人們把寻求使(122)成立的最佳誤差項的問題称做圓内整点問題．

設 $d(n)$ 为 n 的因子个数．和数 $D(x)=\sum_{1\leqslant n\leqslant x} d(n)$ 就等于包含在双曲綫的扇

形

$$uv \leqslant x, \quad u \geqslant 1, \quad v \geqslant 1$$

中的整点 (u, v) 的个数. Dirichlet[67] 首先証明:

$$D(x) = x(\log x + 2\gamma - 1) + O(\sqrt{x}), \tag{123}$$

此处 γ 表 Euler 常数. 寻求使(123)成立的最佳誤差項的問題称为除数問題.

寻求使表示式(122)与(123)成立的最佳誤差項的問題，吸引了几何数論方面的研究工作者的主要注意力.

1903 年，Вороной[241] 首先打破記录，他对除数問題得到了用 $O(x^{\frac{1}{3}}\log x)$ 代替 $O(x^{\frac{1}{2}})$ 的結果; 而在 1906 年, Sierpinski[242] 对圓內整点問題, 成功地用 $O(x^{\frac{1}{3}})$ 代替了 $O(x^{\frac{1}{2}})$.

45. 估計指数和的方法

用 ϑ 表示使

$$A(x) = \pi x + O(x^{\nu})$$

成立的 ν 的下极限. van der Corput 引进了估計指数和的方法, 从而証明了比 $\vartheta \leqslant \frac{1}{3}$ 更好的結果. 这个結果已为很多数学工作者改进. ϑ 的历史可以总結如下表:

$\vartheta\leqslant$	1/3	37/112	37/112
作者姓名	W. Sierpinski	J. G. van der Corput[84]	J. E. Littlewood[243] 与 A. Walfisz

$\vartheta\leqslant$	163/494	27/82	15/46	13/40
作者姓名	A. Walfisz[244]	L. W. Nieland[245]	E. C. Titchmarsh[78]	华罗庚[246]

除数問題的对应发展如下:

$\vartheta\leqslant$	1/3	33/100	27/82	15/46
作者姓名	Г. Ф. Вороной	J. G. van der Corput[74]	J. G. van der Corput[247]	迟宗陶[248] H. E. Richert[249]

另一方面, 对于这两种情形, Hardy[250] 与 Ingham[251] 証明了 $\vartheta \geqslant \frac{1}{4}$, 或者更精确地有

$$\varlimsup_{x\to\infty} \frac{A(x) - \pi x}{x^{\frac{1}{4}} \log^{\frac{1}{4}} x} > 0, \quad \varliminf_{x\to\infty} \frac{A(x) - \pi x}{x^{\frac{1}{4}} \log^{\frac{1}{4}} x} < 0$$

及

$$\varliminf_{x\to\infty} \frac{D(x) - x\log x - (2\gamma - 1)x}{x^{\frac{1}{4}} \log^{\frac{1}{4}} x \log\log x} < 0 < \varlimsup_{x\to\infty} \frac{D(x) - x\log x - (2\gamma - 1)x}{x^{\frac{1}{4}} \log^{\frac{1}{4}} x \log\log x}.$$

关于誤差項的均值，我們有下面的定理：

$$\int_0^x (A(y) - \pi y)^2 dy = \frac{1}{3\pi^2} \frac{16\zeta^3\left(\frac{3}{2}\right)L^2\left(\frac{3}{2}\right)}{\zeta(3)(1+2^{-\frac{3}{2}})} x^{\frac{3}{2}} + O(x^{1+\varepsilon})$$ [252]

及

$$\int_0^x (D(y) - y\log y - (2\gamma - 1)y)^2 dy = cx^{3/2} + O(x\log^5 x)$$ [253].

46. 除数問題的推廣

用 $d_k(n)$ 表示将 n 表成 k 个因子乘积的表法种数，又命

$$D_k(x) = \sum_{n\leqslant x} d_k(n),$$

則有

$$D_k(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \zeta^k(w)\frac{x^w}{w}dw, \quad (c>1).$$

$w=1$ 为一 k 次极点，其上的留数形如 $xP_k(\log x)$，此处 P_k 为一 $k-1$ 次多項式. 我們記

$$D_k(x) = xP_k(\log x) + \Delta_k(x).$$

对于 $k=2$，我們回到了上面研究过的除数問題. 我們相应地定义 α_k 为使

$$\Delta_k(x) = O(x^\vartheta)$$

成立的数 ϑ 的下极限，它的历史一覽表如下：

$$\alpha_k \leqslant \frac{k-1}{k+1}, \quad k=2,3,4,\cdots$$ (Вороной[241], Landau[238]),

$$\alpha_k \leqslant \frac{k-1}{k+2}, \quad k=4,5,\cdots$$ (Hardy-Littlewood[254]),

$$\alpha_7 \leqslant \frac{71}{107},\quad \alpha_8 \leqslant \frac{41}{59},\quad \alpha_9 \leqslant \frac{31}{43},\quad \alpha_{10} \leqslant \frac{26}{35},\quad \alpha_{11} \leqslant \frac{19}{25}$$ (董光昌[255]),

$$\alpha_3 \leqslant \frac{37}{75}$$ (Atkinson[255]),

$$\alpha_k \geqslant \frac{k-1}{2k}$$ (Hardy[250]).

猜想的結果是

$$\alpha_k = \frac{k-1}{2k}.$$

用 β_k 表示 $\Delta_k(x)$ 的平均阶，亦即对任何 $\varepsilon>0$，使

$$\frac{1}{x}\int_0^x \Delta_k^2(y)dy = O(x^{2\beta_k+\varepsilon})$$

成立的最小的数. 显然有

$$\beta_k \leqslant \alpha_k.$$

Titchmarsh[257] 証明了

$$\beta_k \geqslant \frac{k-1}{2k}.$$

又,人們已經証明:

$$\beta_3 = \frac{1}{3}\ (\text{Cramér}^{258)}),\quad \beta_4 \leqslant \frac{23}{54}\ (\text{董光昌}^{255)}),\quad \beta_5 \leqslant \frac{1}{2}^{255)},$$

$$\beta_6 \leqslant \frac{35}{62}^{255)},\qquad \beta_7 \leqslant \frac{11}{18}^{255)}\quad \text{及}\quad \beta_8 \leqslant \frac{149}{230}^{255)}.$$

47. 圓內整点問題的推廣

我們研究 n 維橢球

$$F(u_1, \cdots, u_n) = \sum_{\mu,\ \nu=1}^{n} a_{\mu\nu} u_\mu u_\nu \quad (a_{\mu\nu} = a_{\nu\mu})$$

中的整点个数 $A(x) = A_F(x)$, 此处 $F(u_1, \cdots, u_n)$ 为一具有行列式 D 的正定二次型. 如果存在数 $\alpha(\neq 0)$,使对全体 $\mu, \nu, \alpha a_{\mu\nu}$ 都是整数,則称型 F 为有理的; 否則称 F 为无理的.

用 $V(x) = V_F(x)$ 表示橢球

$$F(u_1, \cdots, u_n) \leqslant x$$

的体积,大家知道

$$V(x) = \pi^{\frac{n}{2}} x^{\frac{n}{2}} \Big/ \sqrt{D}\, \Gamma\left(\frac{n}{2} + 1\right).$$

命

$$P(x) = A_Q(x) - V_Q(x),$$

Landau[259] 証明了

$$P(x) = O(x^{\frac{n}{2} - \frac{n}{n+1}}),$$

$$P(x) = \Omega(x^{\frac{n-1}{4}}).$$

对于 $n \geqslant 8$, 关于有理型 F 的 O-問題, 巳为 Walfisz[260] 完全解决. 对于 $4 \leqslant n \leqslant 7$, Landau[261] 用 Walfisz 方法的一个变形,得到了阶中指数的最优結果. 这就是:如果 F 为有理,則

$$P(x) = O(x^{\frac{n}{2}-1}),\qquad (n > 4),$$

$$P(x) = O(x \log^2 x),\quad (n = 4).$$

Jarník[262] 証明了

$$P(x) = \Omega(x^{\frac{n}{2}-1}).$$

对于 $n=4$, Landau 获得的結果与最后結果只相差一个对数因子. 下面是更精确的結果:

$$P(x) = O(x \log^{\frac{4}{5}} x \log\log x) \quad (\text{Walfisz}^{263)}),$$
$$P(x) = O(x \log^{\frac{2}{3}+\varepsilon} x)^{264)}.$$

設

$$R(x) = \frac{1}{x}\int_0^x |P(y)|dy,$$
$$T(x) = \left(\frac{1}{x}\int_0^x P^2(y)dy\right)^{\frac{1}{2}},$$

Jarník[262] 証明了

a) $$R(x) = \Omega(x^{\frac{n-1}{4}}).$$

b) 对于有理型 F,

$$R(x) = \Omega(x^{\frac{n}{2}-1}).$$

c) 对于 $F = \sum_{i=1}^{n} a_i x_i^2$,

$$R(x) = O(x^{\frac{3}{4}} \log^2 x), \quad n = 2,$$
$$R(x) = O(x^{\frac{1}{2}} \log x), \quad n = 3,$$
$$R(x) = O(x^{\frac{n}{2}-1}), \quad n > 3.$$

d) 如果将 $R(x)$ 换成 $T(x)$, 上列結果仍然正确.

Jarník[265] 証明: 如果 F 的全体系数 $a_{\mu\nu}$ 都是整数, 则有一仅依于 F 的 H, 使

$$\int_0^x P^2(y)dy = Hx^2 \log x + O(x^2 \log^{\frac{1}{2}} x), \quad n = 3,$$
$$\int_0^x P^2(y)dy = Hx^{n-1} + O(g(x)), \qquad n > 3,$$

此处

$$g(x) = x^{\frac{5}{2}} \log x, \quad n = 4,$$
$$g(x) = x^3 \log^2 x, \quad n = 5,$$
$$g(x) = x^{n-2}, \qquad n > 5.$$

对于 $n > 5$, 上之結果已是可能得到的最优結果. 对于 $n = 4$, Walfisz 也得到了此同一結果. Walfisz 也討論了和数

$$\sum_{m \leq x} r^2(m),$$

此处 $r(m)$ 为 $F=n$ 的整数解数. 有关这些問題的結果的詳尽叙述,可在 Walfisz 的标題为"高維橢球中的整点問題 I—IX" 的原始工作中找到.

Jarník 还研究了橢球

$$F=\alpha_1(x_1^2+\cdots+x_\nu^2)+\alpha_2(x_{\nu+1}^2+\cdots+x_n^2).$$

对于 $n=3$, $F=x_1^2+x_2^2+x_3^2$,这就是所謂球內整点問題. 我們用 $x_1=x_2$, $x_2=x_3$, $x_3=x_1$, $x_1=0$, $x_2=0$ 与 $x_3=0$ 等六个平面将球分成 48 个部分, 在每一部分中的整点个数显然相等,我們用 G 表示此数. 截面上的整点都以半数計之,于是因为截面交綫上的整点个数等于 $O(\sqrt{x})$,故有

$$A=48G+O(x^{\frac{1}{2}}).$$

显然

$$G=\sum_{0<x_1\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{3}}}\ \sum_{x_1<x_2\leqslant\sqrt{\frac{1}{2}(x-x_1^2)}}[\sqrt{x-x_1^2-x_2^2}-x_2]+\frac{1}{2}\sum_{0<x_2\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{2}}}([\sqrt{x-x_2^2}]-x_2)+$$

$$+\frac{1}{2}\sum_{0<x_1\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{3}}}([\sqrt{x-2x_1^2}]-x_1)+\frac{1}{2}\sum_{0<x_1\leqslant\frac{x^{\frac{1}{2}}}{\sqrt{3}}}\left(\left[\sqrt{\frac{1}{2}(x-x_1^2)}\right]-x_1\right)+O(x^{\frac{1}{2}}).$$

在建立了[75] Fourier 級数与函数的分数部分間的一个关系后, Виноградов 依靠 van der Corput 引理(第二章, § 8)的帮助,証明了

$$P(x)=O(x^{0.7+\varepsilon}),\quad (\text{Виноградов}^{266)}),$$

$$P(x)=O(x^{0.7-\frac{1}{405}+\varepsilon}),\quad (\text{Виноградов}^{267)}),$$

$$P(x)=O(x^{\frac{11}{16}+\varepsilon}),\quad (\text{Виноградов}^{268)}).$$

又 Szegö[269] 証明了

$$P(x)=\Omega(x^{\frac{1}{2}}\log^{\frac{1}{2}}x).$$

Виноградов 估計球內整点个数的方法, 可以直接用来估計具有負判別式 $-t$ 而 $t\leqslant x$ 的純虛二次型的全体类数之和. 事实上, 这两問題的相互关系类似于二維空間中的圓內整点問題与除数問題的关系.

对于球面上的整点个数的估計, Линник[270] 得到下面的

定理. 設 $m\equiv1,2\pmod 4$ 或 $m\equiv3\pmod 8$;又設 Γ 为球 F_3: $x^2+y^2+z^2=$ $=m$ 上的一个凸球面区域, 它的边界由有限多条光滑曲綫組成. 用 q 表一适合条件 $\left(\frac{-m}{q}\right)=1$ 的奇素数. 命 $H_0(m)$ 与 $H_0(\Gamma)$ 分别表示 F_3 上的与 Γ 中的适合 $(x,y,z)=1$ 的整点个数, 又命 $H(m)$ 与 $H(\Gamma)$ 分别表示 F_3 上的与 Γ 中的整点个数, 則对固定的 q 与 $m\to\infty$,可有

$$H_0(\Gamma) = \frac{\text{mes}\,\Gamma}{4\pi m} H_0(m)\ (1 + K_0(\lambda, m, q)),$$

$$H(\Gamma) = \frac{\text{mes}\,\Gamma}{4\pi m} H(m)\ (1 + K(\lambda, m, q)),$$

此处 mes Γ 表 Γ 的面积；$\lambda > 0$ 为适合 $\frac{\text{mes}\,\Gamma}{4\pi m} > \lambda$ 的任何常数，而对固定的 λ, q 及 $m \to \infty$,有 $K_0(\lambda, m, q) \to 0$ 及 $K(\lambda, m, q) \to 0$.

Малышев[271] 将上述結果推广到某种椭球.

48. 无 k 方因子数的分布

如果一个整数不能被任何大于 1 的整数的 k 次乘冪所整除，就称它为一无 k 方因子的整数. 用 $Q_k(x)$ 表示 $\leqslant x$ 的无 k 方因子整数的个数,则

$$Q_k(x) = \sum_{l^k m \leqslant x} \mu(l) = \sum_{l \leqslant x^{\frac{1}{k}}} \mu(l) \left[\frac{x}{l^k}\right] = x \sum_{l \leqslant x^{\frac{1}{k}}} \frac{\mu(l)}{l^k} + O(x^{\frac{1}{k}}) =$$

$$= \zeta^{-1}(k)x + O(x^{\frac{1}{k}}).$$

这儿的誤差項可用第三章 § 19 的方法加以改进.

又用 $q_k(n)$ 表示第 n 个无 k 方因子数,则当 $n \to \infty$ 时，显然有 $q_k(n) \sim \zeta^{-1}(k)n$ Fogels[141] 証明了

$$q_k(n+1) - q_k(n) = O(n^{\frac{k}{3k-1}+\varepsilon}).$$

这个結果被下述的 Davenport 与 Roth[272] 的結果所代替. 对于任何 $t > 1$,我們有

$$Q_k(x+h) - Q_k(x) = \sum_{x < l^k m \leqslant x+h} \mu(l) =$$

$$= \sum_{1 \leqslant l \leqslant t} \mu(l) \left(\left[\frac{x+h}{l^k}\right] - \left[\frac{x}{l^k}\right]\right) + O\Big(\sum_{\substack{x < l^k m \leqslant x+h \\ l > t}} 1\Big) =$$

$$= \frac{h}{\zeta(k)} + O(t) + O(ht^{1-k}) + O(N),$$

这里的 N 表示适合 $x < l^k m \leqslant x + h$, $l > t$ 的数对 (l, m) 的对数. 关于 N 的估計为

$$O(x^{\frac{1}{2k-1}+\varepsilon}(ht^{-\frac{2k}{2k-1}} + t^{-\frac{1}{2k-1}})).$$

于是

$$q_k(n+1) - q_k(n) = O(n^{\frac{1}{2k}+\varepsilon}).$$

对于 $k = 2$, 这个結果已用 van der Corput 关于指数和的估計加以改善,它的最新結果属于 Richert[273],此即

$$q_2(n+1) - q_2(n) = O(n^{\frac{2}{9}} \log n).$$

Erdös[274] 給出它的下估計，他証明了

$$q_2(n+1)-q_2(n)=\Omega\left(\frac{\log n}{\log\log n}\right).$$

49. 一 般 方 法

Cauchy 积分定理在一般数論間題中的应用源于 Landau[238] 的一个工作。在这工作中，他証明了下面的

定理. 假設：c_ν, l_ν 都是复数；$\alpha \geqslant 0$；α_i, γ_i 为实数；δ_i, β_i 都是正数；μ 与 ν 是 $\geqslant 1$ 的整数；$\lambda_1<\lambda_2<\cdots<\lambda_n<\cdots$：

a) 对于任何 $\varepsilon>0$，都有

$$c_n=O(n^{\alpha+\varepsilon});$$

b) 对于 $\sigma>1+\alpha$，由

$$Z(s)=\sum_{n=1}^{\infty}\frac{c_n}{n^s}$$

定义的函数在全平面上是半純的，且在任何带状区域 $\sigma_1\leqslant\sigma\leqslant\sigma_2$ 中有有限多个极点；

c) $$\sum_{n=1}^{\infty} l_n e^{\lambda_n s}$$

在 $\sigma<0$ 时絕对收斂；

d) 对于 $\sigma<0$，

$$\Gamma(\alpha_1+\beta_1 s)\cdots\Gamma(\alpha_\mu+\beta_\mu s)Z(s)=$$
$$=\Gamma(\gamma_1-\delta_1 s)\cdots\Gamma(\gamma_\nu-\delta_\nu s)\sum_{n=1}^{\infty} l_n e^{\lambda_n s};$$

e) $$\beta_1+\cdots+\beta_\mu=\delta_1+\cdots+\delta_\nu;$$

f) 如命

$$\gamma_1+\cdots+\gamma_\nu-(\alpha_1+\cdots+\alpha_\mu)+\frac{1}{2}(\mu-\nu)=\eta,$$

則有

$$\eta\geqslant\frac{1}{2}\quad 及\quad \eta\geqslant\alpha+\frac{1}{2};$$

g) 对于固定的带状区域 $\sigma_1\leqslant\sigma\leqslant\sigma_2$，存在常数 $\gamma=\gamma(\sigma_1,\sigma_2)$，使对 $\sigma_1\leqslant\sigma\leqslant\sigma_2$ 及大的 $|t|$，有

$$Z(s)=O(e^{\gamma|t|})$$

成立。

結論： 对于任何 $\varepsilon > 0$，有

$$\sum_{n\leqslant x} c_n = R(x) + O(x^{(\alpha+1)\frac{2\eta-1}{2\eta+1}+\varepsilon}),$$

此处 $R(x)$ 为在带状区域

$$(\alpha+1)\frac{2\eta-1}{2\eta+1} < \sigma \leqslant \alpha+1$$

中的 $\frac{Z(s)}{s}$ 的一切可能的极点上函数

$$\frac{x^s}{s} Z(s)$$

的各个留数之和.

由上面的定理，Landau 立刻得到下述結果：

$$\sum_{n\leqslant x} D_k(n) = x(b_{k-1}\log^{k-1}x + \cdots + b_0) + O(x^{\frac{k-1}{k+1}+\varepsilon}) \quad (k \geqslant 2),$$

$$\sum_{\sum\limits_{1\leqslant\mu,\nu\leqslant k} a_{\mu\nu}u_\mu u_\nu \leqslant x} 1 = Ix^{\frac{k}{2}} + O(x^{\frac{k-1}{2}\frac{k}{k+1}+\varepsilon}) \quad (k \geqslant 2),$$

这里的 $\sum\limits_{1\leqslant\mu,\ \nu\leqslant k} a_{\mu\nu}u_\mu u_\nu$ 为一正定型，而 $Ix^{\frac{k}{2}}$ 表示 $\sum\limits_{1\leqslant\mu,\ \nu\leqslant k} a_{\mu\nu}u_\mu u_\nu \leqslant x$ 的体积. 又

$$\sum_{Na\leqslant x} 1 = ax + O(x^{\frac{1}{3}+\varepsilon}),$$

此处 Na 表示虚二次域 K 中的理想数 a 的距.

命 $\chi_1(n), \cdots, \chi_k(n)$ 为 k 个非主特征，則有

$$\sum_{n_1\cdots n_k\leqslant x} \chi_1(n_1)\cdots\chi_k(n_k) = O(x^{\frac{k-1}{k+1}+\varepsilon}).$$

如果在 $\chi_1(n), \cdots, \chi_k(n)$ 中有主特征，則此結果仍然正确，但在右方多添一主項.

重要問題索引

問題	結果	作者	发表年代	
密率問題	假如两个集合的密率之和大于或等于 1，则和集的密率等于 1.	Schnirelmann	1930	§ 1
	假如两个集合的密率之和小于 1，则和集的密率大于或等于这两集合密率的和.	Mann	1942	§ 1
Kloostermann 和	若 $(c, p) = 1$，则 $\left\lvert \sum_{x=1}^{p-1} e^{2\pi i \left(cx + \frac{d}{x}\right)/p} \right\rvert \leqslant 2\sqrt{p}$.	Weil	1948	§ 12
完全指数和	設 p 为一素数，$f(x) = a_k x^k + \cdots + a_1 x$，又設 $p \nmid a_k$，则 $\left\lvert \sum_{x=1}^{p} e^{2\pi i f(x)/p} \right\rvert \leqslant k\sqrt{p}$.	Weil-Carlitz-Uchiyama	1957	§ 12
	設 q 为一 $\geqslant 1$ 的整数，又 $f(x) = a_k x^k + \cdots + a_1 x$ 为一 k 次整系数多項式，并且 $(a_k, \cdots, a_1, q) = 1$，则有 $\left\lvert \sum_{x=1}^{q} e^{2\pi i f(x)/q} \right\rvert \ll q^{1-\frac{1}{k}+\varepsilon}$, 記号 $\ll$ 中所含的常数与 ε 及 k 有关.	华罗庚	1940	§ 13
mod p 的冪剩余	設 n 是 $p-1$ 的一个因子，它不等于 1，则对全体充分大的 p，mod p 的最小正 n 次非剩余 $< p^{\frac{1}{2k}} (\log p)^2, \quad k = e^{\frac{n-1}{n}}$.	Виноградов	1926	§ 14
mod p 的原根	用 $g(p)$ 表示 p 的最小正原根，则有 $g(p) = O(2^{m+1}\sqrt{p})$, 此处 m 为 $p-1$ 的互不相同的素因子个数.	华罗庚	1942	§ 14
素数分布	設 $\pi(x; q, l)$ 为等差級数 $qn + l$ 中不大于 x 的素数个数，则有 $\pi(x; q, l) = \frac{\mathrm{li}\, x}{\varphi(q)} + O\left(xe^{-c(\log x)^{\frac{3}{5}-\varepsilon}}\right)$, 記号 O 中的常数与 q 及 ε 有关.	Виноградов	1958	§ 19 § 22

問　題	結　　　果	作　者	发表年代	
	对于 $q \leqslant (\log x)^u$，u 为任意一数，可有 $$\pi(x;q,l)=\frac{\mathrm{li}\,x}{\varphi(q)}+O(xe^{-c\sqrt{\log x}}),$$ 記号 O 中所含的常数关于 q 为一致。	Page-Siegel-Walfisz	1936	§ 22
	落在区間 $(A, A+x)$ 中的素数个数 $$\leqslant \frac{2x}{\log x}+O\left(\frac{x}{\log^2 x}\cdot\log\log x\right),$$ 記号 O 中所含的常数关于 A 为一致。	Selberg	1947	§ 4
	等差級数 $\equiv l \pmod q$ 中的最小素数等于 $O(q^C)$，此处 C 为一絕对常数。	Линник	1944	§ 22
	$$\pi(x)-\mathrm{li}\,x=\Omega\left(\frac{x^{\frac{1}{2}}}{\log x}\log\log\log x\right).$$	Littlewood	1914	§ 20
相継素数的差距	用 p_n 表第 n 个素数，则 $$p_{n+1}-p_n=O(p_n^{\frac{38}{61}+\varepsilon}).$$	Ingham	1937	§ 21
	对于任何 $\varepsilon>0$，有无限多个 n，使 $$p_{n+1}-p_n \geqslant \left(\frac{1}{3}-\varepsilon\right)\log p_n\cdot\log\log p_n\frac{\log\log\log\log p_n}{(\log\log\log p_n)^2}.$$	Rankin	1938	§ 21
	对于任何 $\varepsilon>0$，有无限多个 n，使 $$p_{n+1}-p_n \leqslant \left(\frac{57}{59}+\varepsilon\right)\log p_n.$$	Rankin	1940	§ 21
Waring問題	用 $G(k)$ 表示最小的整数 s 之能使任何大整数都可表成至多 s 个 k 次乘冪之和者，则 $G(k)\leqslant k(3\log k+9)$, $G(3)\leqslant 7$, $G(4)=16$,　$G(5)\leqslant 23$,　$G(6)\leqslant 36$.	 Виноградов Линник Davenport	 1947 1942 1939	 § 26 § 26 § 26
	用 $g(k)$ 表示最小的整数 s 之能使任何整数都可表成至多 s 个 k 次乘冪之和者，则在 $$\left(\frac{3}{2}\right)^k-\left[\left(\frac{3}{2}\right)^k\right]\leqslant 1-\left(\frac{1}{2}\right)^k\left\{\left[\left(\frac{3}{2}\right)^k\right]+3\right\}$$ 成立时， $$g(k)=2^k+\left[\left(\frac{3}{2}\right)^k\right]-2\quad(k>6).$$	Dickson-Pillai-Niven	1936—1944	§ 28

續

問題	結果	作者	发表年代	
	$g(6)=73$,	Pillai	1940	§ 28
	$19\leqslant g(4)\leqslant 35,\quad 37\leqslant g(5)\leqslant 54$,	Dickson	1933	§ 28
	$g(3)=9$,	Wieferich	1909	Math. Ann. **66**, 95—101, 1909.
	$g(2)=4$	Lagrange	1770	見 L. E. Dickson 著 History of the theory of numbers II (New York) 275—304, 1934.
	当 $s\geqslant\begin{cases}2^k+1, & 1\leqslant k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2.5), & k>10\end{cases}$ 时,能够得到方程 $N=x_1^k+\cdots+x_s^k$ 的解数的漸近公式。	华罗庚	1953	§ 25
Prouhet問題	用 $N(k)$ 表示具有下面性質的最小的 t: 存在 $x_1,\cdots,x_t,y_1,\cdots,y_t$,但 $y_1,\cdots,y_t$ 并非 $x_1,\cdots,x_t$ 的重新排列,它們滿足 $\sum_{i=1}^{t}x_i^h=\sum_{i=1}^{t}y_i^h\quad(1\leqslant h\leqslant k)$. 則有 $N(k)\leqslant\begin{cases}\frac{1}{2}(k^2+3), & 若\ 2\nmid k,\\ \frac{1}{2}(k^2+4) & 若\ 2\mid k.\end{cases}$	Wright	1935	§ 29
	用 $M(k)$ 表示使 $\sum_{i=1}^{t}x_i^h=\sum_{i=1}^{t}y_i^h\quad(1\leqslant h\leqslant k)$, $\sum_{i=1}^{t}x_i^{k+1}\neq\sum_{i=1}^{t}y_i^{k+1}$ 可解的最小的 t, 則 $M(k)\leqslant(k+1)\left(\left[\frac{\log\frac{1}{2}(k+2)}{\log\left(1+\frac{1}{k}\right)}\right]+1\right)$.	华罗庚	1938	§ 29

續

問　題	結　果	作　者	发表年代	
	$M(k)=k+1, \quad (2\leqslant k\leqslant 9).$			A. Gloden, Mehrgradige Gleichungen, Groningen 1944.
Goldbach 問題[275]	每一大奇数都是三个素数的和。	Виноградов	1937	§ 15 § 30
	每一大偶数都是一个素数与一个是有限多个素数乘积的数之和。	Rényi	1947	§ 32
	每一大偶数都是两个乘积数之和，其中一个不超过两个素数的乘积，而另一个则不超过 366 个素数的乘积。	Ricci	1937	§ 3
Waring-Goldbach 問題	当 $s\geqslant\begin{cases}2^k+1, & 1\leqslant k\leqslant 10,\\ 2k^2(2\log k+\log\log k+2.5), & k>10\end{cases}$ 时,能够得到方程 $N=p_1^k+\cdots+p_s^k$ 的解数的漸近公式,这里的 p_i 都是素数。	华罗庚	1953	§ 33
	用 $H(k)$ 表示具有以下性質的最小整数 s; 每一充分大的整数(适合某些条件的)都是 s 个素数的 k 次乘冪之和,則 $H(k)\leqslant c(k)\sim 4k\log k,$ $H(4)\leqslant 15,\quad H(5)\leqslant 25,\quad H(6)\leqslant 37,$ $H(7)\leqslant 55,\quad H(8)\leqslant 75.$	华罗庚	1953	§ 33
圓內整点問題	对于圓 $u^2+v^2\leqslant x$ 中的整点 (u,v) 的个数 $A(x)$, 有 $A(x)=\pi x+O(x^{\frac{13}{40}+\varepsilon})$	华罗庚	1942	§ 45
	$\varliminf_{x\to\infty}\dfrac{A(x)-\pi x}{x^{\frac{1}{4}}\log^{\frac{1}{4}}x}<0<\varlimsup_{x\to\infty}\dfrac{A(x)-\pi x}{x^{\frac{1}{4}}\log^{\frac{1}{4}}x}$	Hardy	1916	§ 11
	$\int_0^x(A(y)-\pi y)^2dy = =\dfrac{1}{3\pi^2}\cdot\dfrac{16\zeta^2\left(\frac{3}{2}\right)L^2\left(\frac{3}{2}\right)}{\zeta(3)(1+2^{-\frac{3}{2}})}x^{\frac{3}{2}}+O(x^{1+\varepsilon}).$	Landau	1924	§ 45

續

問 題	結 果	作 者	发表年代	
除数問題	用 $D(x)$ 表示双曲扇形 $uv \leqslant x,\ u \geqslant 1,\ v \geqslant 1$ 中的整点 (u, v) 的个数,則有 $$D(x) = x(\log x + 2\gamma - 1) + O(x^{\frac{15}{46}+\varepsilon}).$$	迟宗陶, Richert	1950	§ 45
	$\int_0^x (D(y) - y(\log y + 2\gamma - 1))^2 dy = cx^{\frac{3}{2}} + O(x \log^5 x).$	董光昌	1956	§ 45
	$$\varliminf_{x \to \infty} \frac{D(x) - x(\log x + 2\gamma - 1)}{x^{\frac{1}{4}} \log^{\frac{1}{4}} x \log\log x} < 0 < \varlimsup_{x \to \infty} \frac{D(x) - x(\log x + 2\gamma - 1)}{x^{\frac{1}{4}} \log^{\frac{1}{4}} x \log\log x}.$$	Hardy	1916	§ 45
球內整点問題	对于落在球 $$u^2 + v^2 + w^2 \leqslant x$$ 中的整点 (u, v, w) 的个数 $P(x)$,有 $$P(x) = \frac{4}{3}\pi x^{\frac{3}{2}} + O(x^{\frac{11}{16}+\varepsilon}).$$	Виноградов	1955	§ 47
椭球內的整点問題	設 $F(u_1, \cdots, u_n) = \sum_{\mu, \nu=1}^{n} a_{\mu\nu} u_\mu u_\nu$ 为一有行列式 D 的正定型. 如果存在 $\alpha (\neq 0)$,使对全体 μ 与 ν, $\alpha a_{\mu\nu}$ 都是整数,則对 $n \geqslant 8$,有 $$\sum_{F(u_1, \cdots, u_n) \leqslant x} 1 = \frac{\pi^{\frac{n}{2}} x^{\frac{n}{2}}}{\sqrt{D}\, \Gamma\left(\frac{n}{2} + 1\right)} + O(x^{\frac{n}{2}-1}).$$	Walfisz	1924	§ 47
	在上面的假定下,此同一結論对 $5 \leqslant n \leqslant 7$ 也成立.	Landau	1924	§ 47
	在上面的假定下,有 $$\sum_{F(u_1, \cdots, u_n) \leqslant x} 1 - \frac{\pi^{\frac{n}{2}} x^{\frac{n}{2}}}{\sqrt{D}\, \Gamma\left(\frac{n}{2} + 1\right)} = \Omega(x^{\frac{n}{2}-1}).$$	Jarnik	1931	§ 47

参考書籍

H. Bohr und H. Cramér, Die neuere Entwicklung der analytischen Zahlentheorie, Enzyklopädie der mathematischen Wissenschaften mit Einschluß ihrer Anwendungen II, 3, b, Leipzig, 1923—1927.

T. Estermann, Introduction to modern prime number theory, Cambridge tracts, Cambridge University Press, **41**, 1952.

А. О. Гельфонд, Трансцендентные и алгебраические числа, ГИТТЛ., Москва, 1952.

华罗庚,堆垒素数論,科学出版社,1953. (新版,1957. 有俄文本; Аддитивная теория простых чисел, Тр. Матем. ин-та. им. В. А. Стеклова АН СССР, 1947, т. XXII).

I. F. Koksma, Diophantische Approximationen, Springer Verlag, Berlin, 1936.

A. E. Ingham, The distribution of prime numbers, Cambridge tracts, Cambridge University Press, **30**, 1932.

E. Landau, Handbuch der Lehre von der Verteilung der Primzablen, 1 und 2, Leipzig und Berlin, 1909.

E. Landau, Über einige neuere Fortschritte der additiven Zahlentheorie, Cambridge tracts, Cambridge University Press, **35**, 1937.

E. Landau, Vorlesungen Über Zahlen-theorie, Bd. I, II, III, Leipzig, 1927.

E. Landau, Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, 2. Aufl., Leipzig 1927.

H. H. Ostmann, Additive Zahlentheorie, Bd. I, II, Springer-Verlag, Berlin, 1956.

K. Prachar, Primzahlverteilung, Springer Verlag, Berlin-Göttingen-Heidelberg, 1957.

C. L. Siegel, Transcendental numbers, Princeton Univ. Press, 1949.

Н. Г. Чудаков, Введение в теорию L-функций дирихле, ГИТТЛ; Москва-Ленинград, 1947.

E. C. Titchmarsh, The theory of the Riemann Zeta function, Clarendon Press, Oxford, 1951.

P. Turán, Eine neue Methode in der Analysis und deren Anwendungen, Akadémiai Kiadó, Budapest, 1953 (有中譯本: "数学分析中的一个新方法及其应用",郭煥庭譯,見数学进展,2卷, 312—365, 1956.).

И. М. Виноградов, Избранные труды, Изд. АН СССР, Москва, 1952.

И. М. Виноградов, Метод тригонометрических сумм в теории чисел, Тр. Матем. ин-та им. В. А. Стеклова, АН СССР, 1947, XXIII, (有中譯本:"数論中的三角和法". 越民义譯,見数学进展,一卷一期, 3—106, 1955; 英譯本: The method of trigonometrical sums in the theory of numbers,' K. F. Roth 与 A. Davenport 譯, Interscience publishers, London-New York, 1954).

A. Walfisz, Gitterpunkte in mehrdimensionalen Kugeln, Warszawa, 1957.

参 考 資 料

1) L. E. Dickson, History of the theory of numbers, New York, 1, 421, 1934.

2) N. Pipping 核对了命題 (A) 当 $N \leqslant 10^5$ 是正确的。

3) E. Landau, Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion, Proc. of the 5th Inter. Congress of Math., Cambridge, 1, 93—108, 1912.

4) E. Waring, Meditationes algebraicae, Cambridge, 204—205, 1770, 亦見 L. E. Dickson, History of the theory of numbers, New York, 2, 717—729, 1934.

5) D. Hilbert, Beweis für die Darstellbarkeit der Ganzen Zahlen durch eine feste Anzahl n-ter Potenzen, Math. Ann., **67**, 281—300, 1909.

6) Л. Г. Шнирельман, об аддитивных свойствах чисел, Ростов Н/Д, Изв. Донск. Политехн. ин-та. 14: 2—3 (1930), 3—28; Über additive Eigenschaften von Zahlen, Math. Ann., **107**, 649—690, 1933.

7) G. H. Hardy und J. E. Littlewood, Some problems of "Partitio numerorum"; I: A new solution of Waring's Problem, Gött. Nachr. 33—54, 1920; II. Proof that every large number is the sum of at most 21 biquadrates, Math. Z., **9**, 14—27, 1921; III: On the expression of a number as a sum of primes, Acta Math., **44**, 1—70, 1922, IV: The singular series in Waring's Problem and the value of the number G(k), Math. Z., **12**, 161—188, 1922; V. A further contribution to the study of Goldbach's problem, Proc. London Math. Soc. (2); **22**, 46—56, 1923. VI: Further Researches in Waring's Problem, Math. Z., **23**, 1—37. 1925, VII: The number $\Gamma(k)$ in Waring's Problem, Proc. London Math. Soc., **28**, 518—542, 1928.

8) 事实上，这个方法的思想已經在 Hardy 与 Ramanujan 的下述論文中出現过："Asymoptotic formulae in combinatory analysis", Proc. London Math. Soc. (2), **17**, 75—115, 1918.

9) E. Landau, Vorlesungen Über Zahlentheorie, Leipzig, **1**, 183—234, 1927.

10) И. М. Виноградов, Представление нечётного числа суммой трёх простых чисел, ДАН СССР, **15**, 291—294, 1937.

11) К. Г. Бороздкий, К. Вопросу о постоянной И. М. Виноградова, Тру. Тре. Всесоюзного Матем. Съезда, СССР, **1**, 3, 1956.

12) Ю. В. Линник, О густоте нулей L-рядов, ИАН СССР, **10**, 35—46, 1946; Новые доказательство теоремы Гольдбаха-Виноградова, Матем. Сб., **19** (61), 3—8, 1946.

13) L. E. Dickson, History of the theory of numbers, Vol. I. New York, 347—356, 1934.

14) V. Brun, Le cribe d'Eratosthène et le théorème de Goldbach, Videnskabs-selskabet; Kristiania Skrifter I, Mate.-Naturvidenskapelig Klasse, **3**, 1—36, 1920.

15) A. Selberg, On an elementary method in the theory of primes, Norske vid. selsk. Forhdl. 19, Nr. 18, 64—67, 1947.

16) А. И. Виноградов, Новые аддитивные задачи с простыми числами, Тру. Тре. Всесоюзного Матем. Съезда, СССР, **1**, 4, 1956.

17) A. Selberg, The general sieve method and its place in prime number theory, Proc. of international congress of Math., **1**, 286—292, 1950.

18) Ю. В. Линник, "Большое решета", АН СССР, **30**, 290—292, 1941.

19) A. Rényi (А. Реньи), О представлении четных чисел в виде суммы простого и почти простого числа, ИАН СССР, серия матем., **12**, 57—78, 1948.

20) H. Weyl, Über die Gleichverteilung von Zahlen mod. Eins, Math. Ann., **77**, 313—352, 1916.

21) И. М. Виноградов, О суммах Вейля, Матем. сб., **42**, 521—530, 1935.

22) И. М. Виноградов, Избранные труды, Изд. АН СССР, Москва, 1952.

23) 华罗庚，堆垒素数論，科学出版社，1953.

24) И. М. Виноградов, Новая оценка функции $\zeta(1+it)$, ИАН СССР, серия Матем., **22**, 161—164, 1958.

25) E. Prouhet, Comptes Rendus, Paris, **38**, 225, 1851; 亦見 L. E. Dickson, History of the theory of numbers, Vol. **2**, New York, 705—716, 1934.

26) 华罗庚 (L. K. Hua), On the number of solutions of Tarry's Problem, Acta Scientia Sinica, **1**, 1—76, 1953.

27) И. М. Виноградов, Метод тригонометрических сумм в теории чисел, Тру. Матем. ин-та. Им. В. А. Стеклова, XXIII, 1947.

28) H. Davenport, On sums of Positive integral k-th powers, Proc. Royal Soc. London (A), **170**, 293—299, 1939; On Waring's Problem for fourth powers, Ann. of Math., **40**, 731—747, 1939; On Waring's Problem for fifth and sixth powers, Amer. Journ. of Math., **64**, 199—207, 1942.

29) Ю. В. Линник, О разложении больших чисел на 7 кубов, ДАН СССР, **35**, 179—180, 1942.

30) L. E. Dickson, Proof of the ideal Waring theorem for exponents 7—180, Amer. Journ. Math., 58, 521—529, 1936; Solution of Waring's problem, Amer. Journ. Math., **58**, 530—535, 1936.

31) S. S. Pillai, On Waring's problem, Journ. Indian Math. Soc. (2), **2**, 16—44, 1936; On Waring's Problem g(6)=73, Proc. Indian Acad. Sci. (A), **12**, 30—40, 1940.

32) I. Niven, An unsolved case of Waring Problem, Amer. Journ. Math., **66**, 137—143, 1944.

33) C. L. Siegel, Generalization of Waring's problem to algebraic number fields, Amer. Journ. of Math., **66**, 122—136, 1944.

34) J. G. van der Corput, Neue tahlentheoretische Abschätzungen, I: Math. Ann., **89**, 215—254, 1923; II: Math. Z., **29**, 397—426, 1929.

35) А. Я. Хинчин (A. Ja. Chinčin), Zur additiven Zahlentheorie, Матем. сб., **39**, 3, 27—32, 1932.

36) H. B. Mann, A proof of the fundamental theorem on the density of sums of sets of positive integers, Ann. of Math. (2), **43**, 67—78, 1942.

37) E. Artin and P. Scherk, On the sum of two sets of integers, Ann. of Math. (2), **44**, 138—142, 1943.

38) H. H. Ostmann, Additive Zahlentheorie, Bd. I, II, Springer-Verlag, Berlin, 1956.

39) Ю. В. Линник, Элементарное решение проблемы Waring'a по методу Шнирельмана, Матем. сб., **12** (54), 225—230, 1943.

40) 华罗庚，数論导引，第十九章，科学出版社，1957.

41) Н. П. Романов, К проблеме гольдбаха, Томск, Изв. ин. Матем. и тех. ун-та, I. 34—38, 1935. 亦見 Lubelski 作的文摘，見 Zentralblatt für Math. und ihre Grenzgebiete, **11**, 390, 1935.

42) H. Hellbronn, E. Landau und P. Scherk, Alle Grossen ganzen Zahlen lassen sich also Summe von höchstens 71 Primzahlen darstellen, Časopis pro Pěstovani Math. a Fysiky **65**, 117—141, 1936.

43) G. Ricci, Sur la congettura di Goldbach e la costante di Schnirelmann, Boll. Univ. Mat. Ital., **15**, 183—187, 1936; Annali Della R. Scuola Normale Superiore di Pisa (2) **6**, 70—115, 1937.

44) H. Rademacher, Beiträge zur Viggo Brunschen Methode in der Zahlen-Theorie, Abh. Math. Sem. Univ. Hamburg, **3**, 12—30, 1924.

45) T. Estermann, Eine neue Darstellung und neue Anwendungen der Viggo Brunschen Methode, J. reine angew. Math., **168**, 106—116, 1932.

46) А. А. Бухштаб, Новые улучшения в методе эратосфенова решета, Матем. сб., **4** (46), 375—387, 1938. О разложении чётных чисел на сумму двух слагаемых с ограниченным числом простых множителей, ДАН СССР, **29**, 544—548, 1940.

47) A. Selberg, On elementary methods in prime number theory and their limitations, Den 11-te Skandinaviske Matematikerkongress, 13—22, 1952.

48) H. N. Shapiro and J. Warga, On representations of large integers as sum of primes, Part. I, commun. pure appl. Math., **3**, 153—176, 1950.

49) 尹文霖，关于表充分大的整数为素数和，北京大学学报（自然科学），**3**, 323—326, 1956.

50) И. В. Чулановский, Некоторые оценки связанные с новым методом Selberg'a в элементарной теории чисел, ДАН СССР, **63**, 491—494, 1948.

51) 王 元，整值多項式的某些性质，数学进展，3卷3期 (1957)，416—423.

52) P. Kuhn, Neue Abschätzungen auf Grund der Viggo Brunschen Siebmethode, Tolfte Skandinaviske Matematikerkongressen, Lund, 160—168, 1953.

53) G. Ricci, Ricerche aritmetiche sui Polinomi, Rend. Circ. Mat. Palermo, **57**, 433—475, 1933.

54) H. Heilbronn, Über die Verteilung der Primzahlen in Polynomen, Math. Ann., **104**, 794—799, 1931.

55) 王 元，表大偶数为一个不超过三个素数的乘积及一个不超过四个素数的乘积之和，数学学报，6卷3期，500—513，1956.

56) 王 元，表大偶数为一个素数及一个不超过四个素数的乘积之和，数学学报，6卷4期，565—582，1956.

57) 关于素数定理的历史，請参看第三章.

58) A. Selberg, An elementary proof of the prime number theorem, Ann. of Math., **50**, 305—313, 1949.

59) P. Erdös, On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, Proc. Nat. Acad. Sci. USA, **35**, 374—384, 1949.

60) Tikao Tatuzawa and Kanesiroo Iseki, On Selberg's elementary proof of the prime number theorem, Proc. Japan. Acad., **27**, 340—342, 1951.

61) A. Selberg, An elementary proof of the prime number theorem for arithmetic progressions, Canadian J. Math., **2**, 66—78, 1950.

62) H. N. Shapiro, On primes in arithematic progressions. I: Ann. of Math., (2) **52**, 217—230, 1950; II: Ann. of Math., (2) **52**, 231—243, 1950.

63) W. E. Briggs, An elementary proof of a theorem about the representation of primes by quadratic forms, Canadian J. Math., **6**, 353—363, 1954.

64) H. N. Shapiro, An elementary proof of the prime ideal theorem, Comm. Pure. Appl. Math., **2**, 309—323, 1949.

65) W. Forman and H. N. Shapiro, Abstract prime number theorem, Comm. Pure Appl. Math., **7**, 587—619, 1954.

66) C. F. Gauss, De nexu inter multitudinem classium etc. Werke **2**, 269—291, 1863.

67) P. G. Lejeune-Dirichlet, Über die Bestimmung der mittleren Werte in der Zahlentheorie, Abh. Akad. Berlin (Werke **2**, 49—66) 1849, Math. Abh., 69—83.

68) И. М. Виноградов, Основы теории чисел, М.-Л., Гостехиздат, 1944.

69) H. Steinhaus, Sur un théorème de M. V. Jarnik, Colloquium Math., **1**, 1—5, 1948.

70) G. H. Hardy and J. E. Littlewood, The trigonometrical series associated with the elliptic ϑ-function, Acta Math., **37**, 193—239, 1914.

71) P. O. Кузьмин (R. O. Kusmin), Über einige trigonometrische Ungleichungen, J. Soc. Math. Phys. Leningrad, **1**, 233—239, 1927.

72) E. Landau, Über eine trigonometrische Summe, Nachr. Ges. Wiss. Göttingen, 21—24, 1928.

73) J. G. van der Corput, Über Weylsche Summen, Mathematica B, 1—30, 1936—1937.

74) J. G. van der Corput, Verschärfung der Abschätzungen beim Teilerproblem, Math. Ann., **87**, 39—65, 1922.

75) И. М. Виноградов, О распределении дробных долей значений функций двух переменных, Изв. Ленинградского политехи ин-та, **30**, 31—52, 1927.

76) E. C. Titchmarsh, On van der Corput's method and the zeta function of Riemann. I: Quart. J. of Math., Oxford, **2**, 161—173, 1931; II: Quart. J. of Math., Oxford, **2**, 313—320, 1931.

77) E. Phillips, The zeta function of Riemann; Further developments of van der Corput's method, Quart. J. of Math., Oxford, **4**, 209—225, 1933.

78) E. C. Titchmarsh, On Epstein's zeta function, Proc. London Math. Soc. (2), **36**, 485—500, 1934; The lattice points in a Circle, Proc. London Math. Soc. (2), **38**, 96—115. 1935.

79) 閔嗣鶴 (S. H. Min), On the order of $\zeta(1/2+it)$, Trans. Amer. Math. Soc., **65**, 448—472, 1949.

80) И. М. Виноградов, Новый метод решения некоторых общих вопросов теории чисел, Матем. сб., **43**, 9—20, 1936; Новый метод оценки тригонометрических сумм, Матем. сб., **43**,

175—188, 1936.

81) 华罗庚 (L. K. Hua), An improvement of Vinogradov's mean value theorem and several applications, Quart. J. of Math., Oxford, **20**, 48—61, 1949.

82) 华罗庚 (L. K. Hua), On the number of solutions of Tarry's problem, Acta Scientia Sinica, **1**, 1—76, 1952.

83) Ю. В. Линник, (Ju. V. Linnik), On Wyel's sum, Матем. сб., **12**, 28—39, 1943.

84) 华罗庚 (Л. Г. Хуа), Аддитивная теория простых чисел, Тру. Матем. ин-та им. В. А. Стеклова, XXII, 1947.

85) E. C. Titchmarsh, The theory of the Riemann zetafunction, Oxford, 1951.

86) H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Univ. Hamburg, **10**, 325—348, 1934.

87) A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Strasbourg (N. S., Nr. 2), 1—85, 1948.

88) Janichi Igusa, On the theory of algebraic correspondences and its application to the Riemann hypothesis in function fields, J. Math. Soc. Japen **1**, 147—197, 1949.

89) P. Roquette, Arithmetischer Beweis der Riemannschen Vermutung in Kongruenz-funktionenkörpern beliebigen Geschlechts, J. für Math., **191**, 199—252, 1953.

90) A. Weil, Foundations of algebraic geometry, Amer. Math. Soc. Colloquium Pub., **29**, 1947.

91) A. Weil, On some exponential sums, Proc. nat. Acad. Sci. USA. **34**, 204—207, 1948.

92) L. Carlitz and S. Uchiyama, Bounds for exponential sums, Duke Math. J., **24**, 1, 37—41, 1957.

93) H. D. Kloosterman, On the representation of numbers in the form $ax^2+by^2+cz^2+dw^2$, Acta Math., **49**, 407—464, 1926.

94) H. Salié, Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen, Math. Z., **36**, 263—278, 1932.

95) H. Davenport, On certain exponential sums, J. reine u. angew. Math., **169**, 158—176, 1933.

96) L. J. Mordell, On a sum analogous to a Gauss's sum, Quart. J. Math., Oxford, **3**, 161—167, 1932.

97) 华罗庚与閔嗣鶴 (L. K. Hua and S. H. Min), On a double exponential sum, Science Record, **1**, 23—25, 1942; 閔嗣鶴 (S. H. Min), On systems of algebraic equations and certain multiple exponential sums, Quart. J. Math. Oxford, **18**, 133—142, 1947.

98) 华罗庚 (L. K. Hua), On an exponential sum, Journ. of Chinese Math. Soc., **2**, 301—312, 1940.

99) 华罗庚 (L. K. Hua), On exponential sums over an algebraic field, Canadian J. Math., **3**, 44—51, 1951.

100) 見华罗庚的著作[23] 与 Davenport 的著作[95]

101) Ю. В. Линник и А. Реньи, О некоторых гипотезах теории характеров дирихле, ИАН СССР, серия Матем., **11**, 539—546, 1947.

102) G. Pólya, Über die Verteilung der quadratischen Reste und Nichtreste, Göttingen Nachrichten, 21—29, 1918.

103) И. М. Виноградов, О границе наименьшего невычета n-й степени, ИАН СССР, серия Матем., **20**, 47—58, 1926.

104) N. C. Ankeny, The least quadratic non-residue, Ann. of Math., (2) **55**, 65—72, 1952.

105) И. М. Виноградов, О наименьшем корне, ДАН СССР, 7—11, 1930.

106) 华罗庚 (L. K. Hua), On the least primitive root of a prime, Bull. Amer. Math. Soc., **48**, 726—730, 1942.

107) P. Erdös, On the least primitive root of a prime, Bull. Amer. Math. Soc., **51**, 131—132, 1945.

108) P. Turán, *Soviet result in number theory*, Math. Lapok, 243—266, 1950.

109) 华罗庚 (L. K. Hua), On the least solution of Pell's equation, Bull. Amer. Math. Soc., 48, 731—735, 1942.

110) I. Schur, Einige Bemerkungen zu drei vorstehenden Arbeiten des Herrn G. Pólya, Göttingen Nachrichten, 30—36, 1918.

111) Ю. В. Линник (Ju. V. Linnik), On the characters of primes, I, Матем. сб., **16** (58), 101—120, 1945.

112) R. E. A. Paley, A theorem on characters, J. London Math. Soc., **7**, 28—32, 1932.

113) S. Chowla, On the k-Analogue of a result in the theory of the Riemann zeta function, M. Z., **38**, 483—487, 1932.

114) P. T. Bateman, S. Chowla and P. Erdös, Remarks on the size of L(1, χ), Pub. Math., **1**, 165—182, 1950.

115) S. Chowla, A theorem of characters, J. Indian Math. Soc., **19**, 279—284, 1932.

116) И. М. Виноградов, Некоторые обшие теоремы относяшиеся к теории простых чисел, труды тбилисск, Матем. ин-та, **3**, 1—33, 1938; Einige allgemeine Primzahlsätze, Труды тбилисск. Матем. ин-та, **3**, 35—61, 1938. 亦可見华罗庚的著作[23].

117) P. Turán, On Riemann Hypothesis, ИАН СССР, серия Матем., **11**, 197—262, 1947; On certain exponential sums, Proc. Akad. Wet. Amsterdam, **51**, 343—353, 1948; Eine Neue Methode in der Analysis und deren Anwendungen, Akagemiai Kiado, Budapest, 1953.

118) И. М. Виноградов, Распределение квадратичных вычетов и невычетов вида $p+k$ по простому модулю, Матем. сб., **3** (45), 311—320, 1938; Уточнение метода оценки сумм с простыми числами, ИАН СССР, серия матем., **7**, 17—34, 1943; Новое усовершенствование методы оченки двойных сумм, ДАН СССР, **73**, 635—638, 1950; Новый подход к оченке сумм значений $\chi(p+k)$, ИАН СССР, **16**, 197—210, 1952.

119) A. M. Legendre, Essai sur la théorie des nombres, 2nd edition, Paris, 1808; Théorie des nombres, 3rd edition, Paris, 1830.

120) C. F. Gauss, Werke **2**, 2. Aufl. Göttingen, 444—447, 1876.

121) П. Л. Чебышев (P. L. Tschebyschev), Sur la fonction qui detérmine la totalité des nombres premiers inférieurs à une limite donnée, Memoires présentés à L'Académie Impériale des sciences des St. Pétersbourg par divers savants **6**, 141—157, 1848—1851; J. Math. pur. appl. ser. I, **17**, 341—365, 1852; Œuvres, I, 27—48, 1899; Mémoire sur les nombres premiers, Mémoires présentés à L'Académie Impériale des sciences de St. Pétersbourg par divers savants, **7**, 15—33, 1850—1854; J. Math. pur. appl. ser. I, **17**, 366—390; 1852; Œuvres, **1**, 49—70, 1899.

122) J. J. Sylvester, On Tschebyschev's theory of the totality of Prime numbers comprised within given limits, Amer. J. Math., **4**, 230—247, 1881.

123) B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Größe, Ges. Math. Werke und Wissenschaftlicher Nachlaß, 2. Aufl., 145—155, 1892.

124) J. Hadamard, Essai sur l'étude des fonctions données par leur développement de Taylor, J. Math. pur. appl. (4), **8**, 101—186, 1892; Etude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann, J. Math. pur. appl. (4), **9**, 171—215, 1893.

125) J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et des conséquences arithmétiques, Bull. Soc. Math. France **24**, 199—220, 1896.

126) C. J. de la Vallée Poussin, Recherches analytiques sur la théorie des nombres, première partie: La fonction $\zeta(s)$ de Riemann et les nombres. premiers en général, Ann. Soc. Sci. Bruxelles **20**, 183—256, 1896.

127) H. von Mangoldt, Auszug aus einer Arbeit unter dem Titel: Zu Riemanns Abhandlung "Über die Anzahl der Primzahlen unter einer gegebenen Größe", Sitzungsber. d. Preuss. Akad. d. Wiss. 883—896, 1894; Zu Riemanns Abhandlung "Über die Anzahl der Primzahlen unter einer gegebenen Größe", J. reine u. angew. Math. **144**, 255—305, 1895. Zur Verteilung der Nullstellen der Riemannschen Funktion $\xi(t)$, Math. Ann., **60**, 1—19, 1905.

128) R. J. Backlund, Sur les zéros de la fonction $\zeta(s)$ de Riemann, Comptes Rendus, **158**, 1979—1981, 1914; Über die Nullstellen der Riemannschen Zetafunktion, Acta Math., **41**, 345—375, 1918.

129) H. von Koch, Sur la distribution des nombres premiers, Acta Math., **24**, 159—182, 1901.

130) C. J. de la Vallée. Poussin, Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs á une limite donnée, Mémoires couronnes de l'Acad. Roy. des Sci. de Belgique **59**, Nr. 1, 1899—1900.

131) J. E. Littlewood, Researches in the theory of Riemann ζ-function, Proc. London Math. Soc. (2), **20**, XXII—XXVIII, 1922.

132) Н. Г. Чудаков (J. G. Tschndakov), On zeros of Dirichlet's L-functions, Матем. сб., **1** (43), 591—602, 1936; О функциях $\zeta(s)$ и $\pi(x)$, ДАН СССР, 425—426, 1938.

133) E. C. Titchmarsh, On $\zeta(s)$ and $\pi(x)$, Quart. J. Math. Oxford, **9**, 97—108, 1938.

134) B. Rosser, The n-th prime is greater than $n \log n$, Proc. London Math. Soc. (2), **45**, 21—44, 1938; Explicit bounds for some functions of prime numbers, Amer. J. Math. **63**, 211—232, 1941.

135) A. E. Ingham, The distribution of prime numbers, Cambridge tracts, **30**, 1932.

136) J. E. Littlewood, Sur la distribution des nombres Premiers, Comptes Rendus, **158**, 1869—1872, 1914.

137) S. Skewes, On the difference $\pi(x) - \mathrm{li}\,x$ I: J. London Math. Soc., 8, 277—283, 1933; II: Proc. London Math. Soc., (3) 5, 48—70, 1955, 亦可参考 A. E. Ingham, A note on the distribution of Primes, Acta Arith., **1**, 201—211, 1936.

138) E. Schmidt, Über die Anzahl der Primzahlen unter gegebener Grenze, Math. Ann., **57**, 195—204, 1903.

139) G. Pólya, Über das Vorzeichen des Restgliedes im Primzahlsatz, Gött. Nachr. 19—27, 1930.

140) 参看 J. E. Littlewood 的文章[136]，亦可参看 E. Landau, Vorlesungen über Zahlentheorie, Leipzig, II, 123—150, 1927 或 A. E. Ingham, A note on the distribution of primes, Acta Arith, I. 201—211, 1936.

141) A. E. Ingham, On the difference between consecutive primes, Quart. J. Math., Oxford, **8**, 255—266, 1937. 該文的方法已被 Fogels 用来处理数論函数的各种問題，見 On average value of arithmetic functions, Proc. Cambridge Phil. Soc., **37**, 358—372, 1941.

142) H. Cramér, Some theorems concerning prime numbers, Arkiv för Mat., Astr. och Fys. **15**, **5**, 1921.

143) R. A. Rankin, The difference between consecutive prime numbers, J. London math. Soc., **13**, 242—247, 1938. 同时参考 E. Westzynthius, Über die Verteilung der zahlen, die zu den ersten Primzahlen teilerfremd sind, Commentationes Phys.-mat. Soc. Sci. fenn. 5, Nr. 25, 1—37, 1931. P. Erdös, On the difference of consecutive primes, Quart. J. Math., Oxford, 6, 124—128, 1935. 張德馨 (T. H. Chang), Über aufeinanderfolgende Zahlen, von denen jede mindestens einer von n linearen Kongruenzen genügt, deren Moduln die ersten n Primzahlen sind. Schriften Math. Sem. u. Inst. Angew. Math. Univ., **4**, 35—55, 1938.

144) A. E. Western, Note on the magnitude of the difference between successive primes, J. London math. Soc., **9**, 276—278, 1934.

145) R. A. Rankin, The difference between consecutive prime numbers, II: Proc. Cambridge philos. Soc., **36**, 255—266, 1940; The difference between consecutive prime numbers, III: J. London math. Soc., **22**, 226—230, 1947; The difference between consecutive prime numbers, IV: Proc. Amer. math. Soc., **1**, 143—150, 1950; P. Erdös, The difference of consecutive primes, Duke math. J., **6**, 438—441, 1940.

146) O. Ricci, Sull'andamento della differenza di numeri primi consecutivi, Rev. Math. Univ. Parma, **5**, 3—54, 1954.

147) A. Walfisz (А. З. Вальфиш), Изолированные простые числа, ДАН СССР, **90**, 711—713, 1953.

148) K. Prachar, Über ein Resultat von A. Walfisz, Monatsh. Math., **58**, 114—116, 1954.

149) H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, Acta Arith., **2**, 23—46, 1936.

150) A. Selberg, On the normal density of primes in small intervals, and the difference between consecutive primes, Arch. Math. Naturvid., **47**, 87—105, 1943.

151) G. Hoheisel, Primzahlprobleme in der Analysis, Sitzungsber. der Preuß. Akad. d. Wissensch., Phys.-Math. Kl. Berlin, 580—588, 1930.

152) H. Heilbronn, Über den Primzahlsatz von Herrn Hoheisel, Math. Z., **36**, 394—423, 1933.

153) Н. Г. Чудаков (N. Tchndakoff), On the difference between two neighbouring prime numbers,

Матем. сб., **1** (43), 793—814, 1936.

154) P. Turán, Eine neue Methode in der Analysis und deren Anwendungen, Akadémial Kiadó, Budapest 1953. (有中譯本,"数学分析中的一个新方法及其应用",郭焕庭譯,見数学进展,第二卷, 312—365, 1956).

155) H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, Proc. mat.-fiz., **45**, 51—74, 1937; Acta math., **2**, 23—46, 1936.

156) Н. Г. Чудаков, О конечной разности для функции $\psi(x, k, l)$, ИАН СССР, серия матем., **12**, 31—46, 1948; К. А. Родосский, О распределении простых чисел в коротких арифметических прогрессиях. ИАН СССР, серия матем., **12**, 123—128, 1948.

157) A. Page, On the number of primes in an arithmetic progression, Proc. London math. Soc. (2) **39**, 116—141, 1935.

158) Tikao Tatuzawa, On the number of the primes in an arithmetic progression, Japanese J. Math., **21**, 93—111, 1951.

159) C. L. Siegel, Über die Klassenzahl quadratischer Zahlkörper, Acta Arith., **1**, 83—86, 1936.

160) A. Walfisz, Zur additiven Zahlentheorie II, Math. Z., **40**, 592—607, 1936.

161) Ю. В. Линник (U. V. Linnik), On the least prime in an arithmetic progression, I: The basic theorem, Матем. сб., **15** (57), 139—178, 1944; II: The Deuring-Heilbronn's phenomenon, Матем. сб., **15** (57), 347—368, 1944.

162) К. А. Родосский, О наименьшем простом числе в арифметической прогрессии и нулях L-функций, ДАН СССР, **88**, 753—756, 1953; О наименьшем простом числе в арифметической прогрессии, Матем. сб., **34** (76), 331—356, 1954.

163) S. Chowla, On the least prime in an arithmet. Progression, J. Indian math. Soc., **1**, 1—3, 1934.

164) P. Turán, Über die Primzahlen der arithmetischen Progression, Acta Litt. Sci. Szeged 8, 226—235, 1937.

165) P. Erdös, On some applications of Brun's method, Acta Univ. Szeged. Sect. Sci. Math., **13**, 57—63, 1949.

166) Hans-Egon Richert, Über quadratfreie Zahlen mit genau r Primfaktoren in einer arithmetischen Progression, J. reine u. angew. Math., **192**, 180—203, 1953.

167) И. И Пятецкий-Шапиро, О распределении простых чисел в последовательностях вида $|f(n)|$, Матем. сб., **33** (75), 559—566, 1953.

168) E. Landau, Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes, Math. Ann., **56**, 645—670, 1903; Über ideale und Primidale in Idealklassen, Math. Z., **2**, 52—154, 1918.

169) А. А. Бухштаб, Асимптотическая оценка одной общей теоретико-числовой функции, Матем. сб., **2**, 1239—1245, 1937.

170) S. Chowla and T. Vijayaraghaven, On the largest prime divisors of numbers, J. Indian math. Soc., **11**, 31—37, 1947.

171) А. А. Бухштаб. О числах арифметической прогрессии у которых все простых множители малы по порядку роста, ДАН СССР, **67**, 5—8, 1949.

172) 华罗庚 (L. K. Hua), 一个求极限的問題, 中国科学, **2**, 393—402, 1951.

173) 閔嗣鶴 (S. H. Min), 談一个求极限的問題, 数学学报, **4**, 381—384, 1954.

174) N. G. de Bruijn, On the number of uncancelled elements in the sieve of Eratosthenes, Indag. math., **12**, 247—256, 1950; The asymptotic behaviour of a function occurring in the theory of primes, J. Indian math. Soc., **15**, 25—32, 1951.

175) А. А. Бухштаб, Об асимптотической оценке числа чисел арифметической прогрессии неделящихся на "относительно" малые простые числа, Матем. сб., **28**, 165—184, 1951.

176) N. G. de Bruijn, On the number of positive integers $\leqslant x$ and free of prime factors $>y$, Nederl. Akad. Wet., Proc., Ser. A 54, 50—60, Indagat. math., **13**, 50—60, 1950. 同时参考 Ramaswami, The number of positive integers $\leqslant x$ and free of prime divisors $>x^c$ and a problem of S. S. Pillai, Duke math. J., **16**, 99—109, 1949; Number of integers in a assigned A. P., $\leqslant x$ and prime to primes greater than x^c, Proc. Amer. math. Soc., **2**, 318—319, 1951.

177) 华罗庚 (L. K. Hua), On Waring's problem, Quart. J. Math., Oxford, **9**, 199—202, 1938.

178) 这个結果稍优于 Виноградов 原来的結果: $s \geqslant [10 k^2 \log k]$.

179) P. Erdös, On the representation of an integer as the sum of k k-th powers, J. London math. Soc., **11**, 133—136, 1936.

180) S. Chowla and S. S. Pillai, The number of representations of a number as a sum of n non-negative n-th powers, Quart. J. Math., Oxford, **7**, 56—59, 1936.

181) K. Mahler, Note on hypothesis K of Hardy and Littlewood, J. London math. Soc., **11**, 136—138, 1936.

182) G. L. Watson, A proof of the seven cube theorem, J. London math. Soc., **26**, 153—156, 1951.

183) 例如 F. Hausdorff, Math. Ann., **67**, 301—305, 1909; E. Stridsberg, Math. Ann., **72**, 145—152, 1912.

184) 华罗庚 (L. K. Hua), On a generalized Waring problem, Proc. London. Math. Soc. (2), **43**, 161—182, 1937.

185) R. E. Huston, Asymptotic generalizations of Warings theorem, Proc. London math. Soc., **39**, 82—115, 1935.

186) 华罗庚 (L. K. Hua), On Waring problem with polynomial summands, Amer. J. Math., **58**, 553—562, 1936; On a generalized Waring problem, Proc. London math. Soc. (2) **43**, 161—182, 1937; On a generalized Waring problem, II, Journ. Chinese Math. Soc. **2**, 175—191, 1940.

187) 华罗庚 (L. K. Hua), On Waring problem with cubic polynomial summands, J. Indian math. Soc., **4**, 127—135, 1940.

188) В. И. Нечаев, О представлении натуральных чисел суммой слагаемых вида $\frac{x(x+1)\cdots(x+k-1)}{k!}$, ИАН СССР, **17**, 485—498, 1953.

189) 华罗庚 (L. K. Hua)[23], 同时参考 S. S. Pillai, On Warings problem VI (polynomial summands), J. Annamalai Univ., **6**, 171—197, 1937.

190) K. F. Roth, A problem in additive number theory, Proc. London math. Soc. (2) **53**, 381—395, 1951.

191) E. M. Wright, An extension of Warings problem, Philos. Trans. Roy. Soc. London **232**, 1—26, 1933; Proportionality conditions in Warings problem, Math. Z. **38**, 730—746, 1934.

192) F. C. Auluck and S. Chowla, The representation of a large number as a sum of "almost equal" squares, Proc. Indian Acad. Sci., Sect. A. **6**, 81—82, 1937. 同时参考 E. M. Wright, The representation of a number as a sum of four "almost proportional" squares, Quart. J. Math., Oxford, **7**, 230—240, 1936.

193) Б. И. Сегал, Об одной теореме, аналогичной теореме Варинга, ДАН СССР, Новая серия, **2**, 47—49, 1933.

194) S. Chowla, A theorem on irrational indefinite quadratic forms, J. London math. Soc. **9**, 162—163, 1934.

195) H. Davenport and H. Heilbronn, On indefinite quadratic forms in five variables, J. London math. Soc. **21**, 185—193, 1946.

196) H. Davenport and K. F. Roth, The solubility of certain Diophantine inequalities, Mathematica **2**, 81—96, 1955.

197) A. Oppenheim, Values of quadratic forms, III. Monatsh. Math. **57**, 97—101, 1933.

198) L. E. Dickson, Recent progress on Waring theorem, Bull. Amer. math. Soc. **39**, 701—727, 1933.

199) S. S. Pillai, Waring's problem with indices $\geqslant n$, Proc. Indian. Acad. Sci. (A) **12**, 41—45, 1940. 同时参考 M. Haberzetle, The Waring problem with summands x^m, $m \geqslant n$, Duke math. J. **5**, 49—57, 1939.

200) E. M. Wright, On Tarry's problem, Quart. J. Math., Oxford, **6**, 261—267, 1935.

201) 华罗庚 (L. K. Hua), On Tarry's problem, Quart. J. Math., Oxford, **9**, 315—320, 1938. 同时参考 E. M. Wright, On Tarry's problem III, Quart J. Math., Oxford, **8**, 48—50, 1937.

202) 华罗庚 (L. K. Hua), Improvement of a result of Wright, J. London Math. Soc. **24**, 157—159, 1943.

203) К. К. Марджанишвили, Об одновременном представлении и чисел суммами полных первых, вторых, ··· n-ых степеней, ИАН СССР, серия матем., **1**, 609—631, 1937; О некоторых нелинейных системах уравнений в целых числах, Матем. сб., **33**, 639—675, 1953.

204) T. Estermann, A new result in the additive prime-number theory, Quart. J. Math., Oxford, 8, 32—38, 1937.

205) T. Estermann, Proof that every large integer is the sum of two primes and a square, Proc. London math. Soc. **11**, 501—516, 1937.

206) Ю. В. Линник, О возможности единого метода в некоторых вопросах "аддитивной" и "дистрибутивной" теории простых чисел, ДАН СССР, **49**, 3—7, 1945.

207) Н. Г. Чудаков (N. Tchudakoff), On Goldbach-Vinogradov's theorem, Ann. of Math. (2) **48**, 515—545, 1947.

208) C. B. Haselgrove, Some theorems in the analytic theory of numbers, J. London Math. Soc. **26**, 273—277, 1951.

209) R. D. James and H. Weyl, Elementary note on prime-number problems of Vinogradov's type, Amer. J. Math. **64**, 539—552, 1942.

210) Hans-Egon Richert, Aus der additiven Primzahltheorie, J. für Math. **191**, 179—198, 1953.

211) J. G. Van der Corput, Propriétés additives, Acta Arithm. **3**, 181—234, 1939.

212) A. Zulauf, Beweis einer Erweiterung des Satzes von Goldbach-Vinogradov, J. reine angew. Math. **190**, 169—198, 1952.

213) 吳 方 (Wu Fang), 素数变数的綫性方程組, 数学学报, **7**, 102—121, 1957.

214) J. G. Van der Corput, Sur l'hypothese de Goldbach pour presque tous les nombres pairs, Acta Arithm. **2**, 266—290, 1937.

215) Н. Г. Чудаков, О проблеме гольдбаха, ДАН СССР, **17**, 331—334, 1937.

216) T. Estermann, Proof that almost all even positive integers are sums of two primes, Proc. London math. Soc. (1) **44**, 307—314, 1938.

217) H. Heilbronn, 見 Zentralblatt für Mathematik und ihre Grenzgebiete, **16**, 291—292, 1937.

218) 华罗庚 (L. K. Hua), Some results in the additive prime number theory, Quart. J. Math., Oxford, **9**, 68—80, 1938.

219) Ю. В. Линник, Некоторых уисловные теоремы, касающиеся бинарных задач с простыми числами, ДАН СССР, **77**, 15—18, 1951; Некоторых условные теоремы касающиеся бинарной проблемы Гольдбаха, ИАН СССР, **16**, 503—520, 1952.

220) Ю. В. Линник, Складывание простых чисел со степенями одного и того же числа, Матем. сб., **32**, 3—60, 1953.

221) А. А. Бухштаб, Об одном аддитивном представлении целых чисел, Матем. сб., **10**, (52), 1—2, 87—91, 1942.

222) 华罗庚 (L. K. Hua)[23] 也見 И. М. Виноградов, Einige allgemeine Primzahlsätze. Труды Тбилисск. Матем. Института, **3**, 35—67, 1938; 华罗庚, On the representation of numbers as the sum of powers of primes, Math. Z. **44**, 335—346, 1938; S. Pillai, On Waring's problem with powers of primes, Proc. Indian Acad. Sci., Sect. A **12**, 202—204, 1940.

223) H. Halberstam, Representation of integers as sums of a square of a prime and a cube of a prime and a cube, Proc. London math. Soc. (2) **52**, 455—466, 1951.

224) K. Prachar, Über ein problem vom Waring-Goldbachschen Typ. I. Monatsh. Math. **57**, 66—74, 1953; Über ein problem vom Waring-Goldbachschen Typ. II, Monatsh. Math. **57**, 113—116, 1953.

225) И. И. Шапиро-Пятецкий, Об одном варианте проблемы Варинга-Гольдбаха, Матем. сб., **30**, 105—120, 1952.

226) К. К. Марджанишвили, Об одной задаче аддитивной теории чисел, ИАН СССР, серия матем., **4**, 193—214, 1940.

227) J. G. Van der Corput, Diophantische Ungleichungen I, zur Gleichverteilung modulo Eins, Acta math., **56**, 373—456, 1931.

228) I. F. Koksma, Ein mengentheoretischer Satz über die Gleichverteilung modulo Eins, Compositio math., **2**, 250—258, 1935.

229) И. М. Виноградов, Аналитическое доказательство теоремы о распределении дробных

частей целого многочлена, ИАН СССР, серия матем. (6), **21**, 567—578, 1927.

230) I. F. Koksma, Diophantische Approximationen, Springer-Verlag, Berlin 1936.

231) P. Erdös and P. Turán, On a problem in the theory of uniform distribution, I, Proc. Akad. Wet. Amsterdam 1146—1154, 1948.

232) T. Van Aardenne-Ehrenfest, On the impossibility of a just distribution, Proc. Akad. Wet. Amsterdam **52**, 734—739, 1949.

233) И. М. Виноградов, Об оценке тригонометрических сумм с простыми числами, ИАН СССР, серия матем., **12**, 225—248, 1948.

234) P. Turán, Über die Primzahlen der arithmetischen Progression, Acta Litt. Sci. Szeged **8**, 226—235, 1937.

235) А. Г. Постников, К вопросу о распределении дробных долей показательной функции, ДАН СССР, **86**, 473—476, 1952; И. И. Шапиро-Пятечкий, О законах распредерения дробных долей показательной функции, ИАН СССР, Серия матем. **17**, 49—52, 1951.

236) Н. М. Коробов, О некоторых вопросах равномерного распределения, ИАН СССР, серия матем., **14**, 215—238, 1950.

237) Н. М. Коробов, Многомерные задачи распределения дробных долей, ИАН СССР, серия матем., **17**, 389—400, 1953; Дробные доли показательных функчий, Труды матем. института им. Стеклова. АН СССР, **38**, 87—96, 1951; О дробных долях показательных функций, УМН, СССР, **6**, 151—152, 1951.

238) E. Landau, Über die Anzahl der Gitterpunkte in gewissen Bereichen, Gött. Nachr. 687—771, 1912.

239) A. Oppenheim, Some identities in the theory of numbers, Proc. London math. Soc. (2) **26**, 295—350, 1927.

240) V. Jarník, Über Gitterpunkte in der Ebene, Rozpravy **33**, 36, 1924.

241) Г. Вороной (G. Voronoi), Sur un problème du calcul des fonctions asymptotiques, J. für Math. **126**, 241—282, 1903.

242) W. Sierpinski, O pewnem zagadnienise z rachunku funkcyj asymptotycznych, Prace Mat.-Fiz. **17**, 77—118, 1906.

243) I. E. Littlewood and A. Walfisz, The lattice points of a circle, Proc. Royal Soc. London, Ser. (A) **106**, 478—488, 1925.

244) A. Walfisz, Teilerprobleme, Math. Z. **26**, 66—88, 1927.

245) L. W. Nieland, Über das Kreisproblem, Math. Ann. **98**, 717—736, 1928.

246) 华罗庚 (L. K. Hua), The lattice points in a circle, Quart. J. Math., Oxford, **13**, 18—29, 1942.

247) I. G. Van der Corput, Zum Teilerproblem, Math. Ann. **98**, 697—716, 1928.

248) 迟宗陶 (T. T. Chih), The Dirichlet's divisor problem, Science Report of Tsing Hua Univ., 402—427, 1950.

249) H. E. Richert, Verschärfung der Abschätzung beim Dirichletschen Teilerproblem Math. Z. **58**, 204—218, 1953.

250) G. H. Hardy, On Dirichlet's divisor problem, Proc. London math. Soc. **15**, 1—25, 1916.

251) A. E. Ingham, On the classical lattice point problems, Proc. Cambridge philos. Soc. **36**, 131—138, 1940. P. Erdös 与 W. H. J. Fuchs 用一初等方法得到了一个精确性稍差但更一般的結果，見 On a problem of additive number theory, Lond. Math. Soc. **31**, 67—73, 1956.

252) E. Landau, Über die Gitterpunkte in einem Kreise IV, Gött. Nachr., 58—65, 1924.

253) 董光昌 (K. C. Tong), 除数問題 (III), 数学学报, **6**, 515—541, 1956.

254) G. H. Hardy and I. E. Littlewood, The approximate functional equation in the theory of the zeta-function, with applications to the divisor problems of Dirichlet and Piltz, Proc. London math. Soc. (2) **21**, 39—74, 1922.

255) 董光昌 (K. C. Tong), 除数問題，数学学报，**2**, 258—266, 1952.

256) F. V. Atkinson, A divisor problem, Quart. Journ. Math. (Oxford), **12**, 193—200, 1941.

257) E. C. Titchmarsh, On divisor problems, Quart. J. Math., Oxford, **9**, 216—220, 1938.

258) H. Cramér, Über das Teilerproblem von Piltz, Arkiv für Mat., Astr. och Fysik **16**, 21,

1922.

259) E. Landau, Zur analytischen Zahlentheorie der definiten quadratischen Formen (Über die Gitterpunkte in einem mehrdimensionalen Ellipsoid), Berliner Akademieberichte, 458—476, 1915. Über eine Aufgabe aus der Theorie der quadratischen Formen, Wiener Akademieberichte, **124**, 445—468, 1915. Über die Anzahl der Gitterpunkte in gewissen Bereichen IV, Gött. Nachr., 137—150, 1924.

260) A. Walfisz, Über Gitterpunkte in mehrdimensionalen Ellipsoiden, Math. Z. **19**, 300—307, 1924.

261) E. Landau, Über Gitterpunkte in mehrdimensionalen Ellipsoiden, Math. Z. **21**, 126—132, 1924.

262) V. Jarník, Über die Mittelwertsätze der Gitterpunktlehre I, Math. Z. **33**, 62—84, 1931.

263) A. Walfisz, Über Gitterpunkte in mehrdimensionalen Ellipsoiden, VIII, Acad. Sci. URSS. Trav. Inst. math. Thilissi, **5**, 181—196, 1939.

264) 这个結果能用 Виноградов[24] 的方法証得.

265) V. Jarník, Über die Mittelwertsätze der Gitterpunktlehre, V, Casopis Mat. Fysik., Praha, **69**, 148—174, 1940.

266) И. М. Виноградов, Число целых точек в шаре, Труды Матем. Института им. В. А. Стеклова, **9**, 17—38, 1935.

267) И. М. Виноградов, Улучшение остаточного члена одной асимптотической формулы, ИАН СССР, серия матем., **13**, 97—110, 1949.

268) И. М. Виноградов, Улучшение асимптотических формул для числа целых точек в области трех измерений, ИАН СССР, серия матем., **19**, 3—9, 1955.

269) G. Szegö, Beiträge zur Theorie der Laguerreschen Polynome II, Zahlentheoretische Anwendungen, Math. Z. **25**, 388—404, 1926.

270) Ю. В. Линник, Асимптотическое распределение целых точек на сфере, ДАН СССР, **96**, 909—912, 1954.

271) А. В. Малышев, Асимптотическое распределение целых точек на некоторых эллипсоидах, труды третьего всесоюзного математического съезда АН СССР, 7—8, 1956.

272) H. Davenport and K. F. Roth, On the gaps between consecutive k-free integers, J. London math. Soc. **26**, 268—273, 1951.

273) H. E. Richert, On the difference between consecutive squarefree numbers, J. London math. Soc. **29**, 16—20, 1954, 同时参考 K. F. Roth, On the gaps between square-free numbers, J. London Math. Soc. **26**, 263—268, 1951.

274) P. Erdös, Some problems and results in number theory, Publ. Math. Debrecen, **2**, 103—109, 1951.

275) 由于相似性，故未将孿生素数問題的結果列入表內.

附　　录

1. 篩法及其应用

1957 年,王元[1]証明了下面的結果:

定理 1. 每一充分大的偶数都能表成一个不超过 2 个素数的乘积与一个不超过 3 个素数的乘积之和.

命 p_i 表示第 i 个奇素数. 給出偶数 x 及实数 ξ. 命

$$a;\quad a_i,\quad b_i \tag{ω}$$

为适合下面条件的整数集合:

$a=0$ 或 1, $0\leqslant a_i$, $b_i<p_i$, 若 $p_i|x$, 則 $a_i=b_i$,否則

$$a_i \neq b_i \quad (1\leqslant i\leqslant r), \tag{1}$$

此处 $p_r\leqslant\xi<p_{r+1}$. 命 $F_\omega(x,\xi)$ 为适合下面条件的整数 n 的个数:

$$1\leqslant n\leqslant x,\quad n\equiv a(\bmod 2),\quad n\not\equiv a_i\ (\bmod p_i),$$

$$n\not\equiv b_i\ (\bmod p_i)\quad (1\leqslant i\leqslant r), \tag{2}$$

則由 Brun–Бухштаб–Selberg 方法(見 § 3)可知,存在非負递增且仅有有限多个不連續点的函数 $\lambda(z)$ 及 $\Lambda(z)$ $(1<z\leqslant c)$,使对 (ω) 与 z 一致地有

$$\lambda(z)\frac{c_x x}{\log^2 x}+O\left(\frac{c_x x}{\log^2 x\log\log x}\right)\leqslant F_\omega(x,x^{\frac{1}{z}})\leqslant$$

$$\leqslant\Lambda(z)\frac{c_x x}{\log^2 x}+O\left(\frac{c_x x}{\log^2 x\log\log x}\right), \tag{3}$$

此处 $c_x=2e^{2\gamma}\prod\limits_{p>2}\left(1-\dfrac{1}{(p-1)^2}\right)\prod\limits_{\substack{p|x\\p>2}}\dfrac{p-1}{p-2}$.

定理 1 的証明依賴于下面的引理.

引. 命 $\lambda(z)$ 与 $\Lambda(z)$ 为适合 (3) 的兩个函数, $c>v>u>1$ 为給定的兩数. 若

$$\lambda(v)-\frac{2}{m+1}\int_{u-1}^{v-1}\Lambda\left(\frac{vz}{z+1}\right)\frac{z+1}{z^2}dz>0,$$

則当 x 充分大时,在区間 $1<n<x-1$ 中存在整数 n,使 $n(x-n)$ 不能被 $\leqslant x^{\frac{1}{v}}$ 的素数整除,同时它又最多被区間 $x^{\frac{1}{v}}<p\leqslant x^{\frac{1}{u}}$ 中的 m 个素数整除.

証. 命 $\mathfrak{M}$ 表示适合下面条件的整数 $n(x-n)$ 的集合:

$$1 \leqslant n \leqslant x, \quad n(x-n) \not\equiv 0 \pmod 2, \quad n(x-n) \not\equiv 0 \pmod{p_i}$$

$$(1 \leqslant i \leqslant s), \quad n(x-n) \not\equiv 0 \pmod{p_{s+j}^2} \quad (1 \leqslant j \leqslant t-s), \tag{5}$$

此处 $p_s \leqslant x^{\frac{1}{v}} < p_{s+1}$, $p_t \leqslant x^{\frac{1}{u}} < p_{t+1}$.

記 $\mathfrak{M}$ 的元素个数为 $M(x, x^{\frac{1}{v}}, x^{\frac{1}{u}})$.

取 $a=1$,若 $p_i|x$,則 $a_i=b_i=0$. 否則

$$a_i=0,\ b_i \equiv x \pmod{p_i}, \quad i=1,2,\cdots, \tag{$\bar{\omega}$}$$

則

(i) $F_{\bar{\omega}}(x, x^{\frac{1}{v}}) - M(x, x^{\frac{1}{v}}, x^{\frac{1}{u}}) \leqslant \sum\limits_{x^{\frac{1}{v}}<p\leqslant x^{\frac{1}{u}}} \sum\limits_{\substack{1\leqslant n\leqslant x \\ n(x-n)\equiv 0 \pmod{p^2}}} 1 =$

$$= O(x^{1-\frac{1}{v}}) + O(x^{\frac{1}{u}}).$$

(ii) 存在适合(1)的諸整数列 (ω_j) $(1 \leqslant j \leqslant t-s)$,使 $\mathfrak{M}$ 中至少被 l 个 p_{s+j} 整除的 $n(x-n)$ 的个数不超过

$$\frac{2}{l} \sum_{\substack{1\leqslant j\leqslant t-s \\ p_{s+j}\nmid x}} F_{\omega_j}\left(\frac{x}{p_{s+j}}, x^{\frac{1}{v}}\right) + O(x^{1-\frac{1}{v}}).$$

事实上,記 $\mathfrak{M}$ 中能被 p_{s+j} 整除的元素的集合为 Γ_j, 則当 $p_{s+j}|x$ 时,Γ_j 的元素个数不超过 $\sum\limits_{\substack{n\leqslant x \\ n\equiv 0 \pmod{p_{s+j}}}} 1 = O(x^{1-\frac{1}{v}})$. 又当 $p_{s+j}\nmid x$ 时,命

$a=1$; 当 $p_i|x$ 时, $a_i=b_i=0$,否則

$$a_i=0,\ b_i p_{s+j} \equiv x \pmod{p_i} \quad (1 \leqslant i \leqslant s), \tag{ω_j}$$

則 Γ_j 的元素个数不超过 $2F_{\omega_j}\left(\frac{x}{p_{s+j}}, x^{\frac{1}{v}}\right)$.

若 $n(x-n) \in \mathfrak{M}$ 且至少被 l 个 p_{s+j} 整除,則 $n(x-n)$ 至少属于 l 个类 Γ_j. 故明所欲証.

(iii) 由(i),(ii)可知,当 x 充分大时,$\mathfrak{M}$ 中最多被 m 个 p_{s+j} 整除的元素的个数不少于

$$M(x, x^{\frac{1}{v}}, x^{\frac{1}{u}}) - \frac{2}{m+1} \sum_{\substack{1\leqslant j\leqslant t-s \\ p_{s+j}\nmid x}} F_{\omega_j}\left(\frac{x}{p_{s+j}}, x^{\frac{1}{v}}\right) + O(x^{1-\frac{1}{v}}) =$$

$$= F_{\bar{\omega}}(x, x^{\frac{1}{v}}) - \frac{2}{m+1} \sum_{\substack{1\leqslant j\leqslant t-s \\ p_{s+j}\nmid x}} F_{\omega_j}\left(\frac{x}{p_{s+j}}, x^{\frac{1}{v}}\right) + O(x^{1-\frac{1}{v}}) + O(x^{\frac{1}{u}}) \geqslant$$

$$\geqslant \left(\lambda(v) - \frac{2}{m+1}\int_{u-1}^{v-1} \Lambda\left(\frac{vz}{z+1}\right)\frac{z+1}{z^2}dz\right)\frac{c_x x}{\log^2 x} + O\left(\frac{c_x x}{\log^2 x \log\log x}\right) >$$

$$> 3.$$

换句話說，当 x 充分大时，在区間 $1 < n < x - 1$ 中，存在整数 n 使 $n(x-n)$ 不能被 $\leqslant x^{\frac{1}{v}}$ 的素数整除，同时它又最多被区間 $x^{\frac{1}{v}} < p \leqslant x^{\frac{1}{u}}$ 中 m 个素数整除. 故得引理.

經过計算得

$$\lambda(8) - \frac{2}{3}\int_{\frac{9}{7}}^{7} \Lambda\left(\frac{8z}{z+1}\right)\frac{z+1}{z^2}dz > 0.43.$$

故由引理即得定理 1.

类似地，取 $\mathfrak{M}$ 为适合下面条件的素数 p 的集合:

$$\begin{aligned} 2 < p < x, \quad x - p \not\equiv 0 \,(\bmod\, p_i) \quad (1 \leqslant i \leqslant s), \\ x - p \not\equiv 0 \,(\bmod\, p_{s+j}^2) \quad (1 \leqslant j \leqslant t - s), \end{aligned} \tag{7}$$

則在广义 Riemann 猜想下，王元[2]証明了

定理 2. 在广义 Riemann 猜想下，每一充分大的偶数都是一个素数及一个素因子个数不超过 3 的整数之和.

在定理 2 的証明过程中可以看到，广义 Riemann 猜想可以用

$$\sum_{\mathscr{D} \leqslant x^{\frac{1}{2}-\delta}} \mu^2(\mathscr{D}) \operatorname*{Max}_{\substack{l \,(\bmod\, \mathscr{D}) \\ (l,\mathscr{D})=1}} \left| \pi(x, \mathscr{D}, l) - \frac{\operatorname{li} x}{\varphi(\mathscr{D})} \right| = O\left(\frac{x}{\log^A x}\right) \tag{8}$$

来代替，此处 δ 为任何給定的正数，A 为任何正常数，而与 O 有关的常数仅依賴于 δ 及 A.

(8)式也可以換成

$$\sum_{\mathscr{D} \leqslant x^{\frac{1}{2}-\delta}} \mu^2(\mathscr{D}) \operatorname*{Max}_{\substack{l \,(\bmod\, \mathscr{D}) \\ (l,\mathscr{D})=1}} \left| P(x, \mathscr{D}, l) - \frac{x}{\varphi(\mathscr{D}) \log x} \right| = O\left(\frac{x}{\log^A x}\right), \tag{9}$$

此处 $P(x, \mathscr{D}, l) = \sum\limits_{\substack{1 < p \leqslant x \\ p \equiv l \,(\bmod\, \mathscr{D})}} e^{-\frac{\log x}{x} p} \log p.$

运用 Линник 的大篩法及 Dirichlet L 函数的零点的密度定理，Барбан[3]首先証明了(8)式当 $\delta < \frac{1}{6}$ 时成立. 潘承洞[4]独立地証明了(9)式当 $\delta < \frac{1}{3}$ 时成立. 并由此推出

定理 3. 每一充分大的偶数为一个素数及一个不超过 5 个素数的乘积之和.

王元[5] 又将定理 3 中的 5 改进为 4 .

此外，王元[6] 还証明了

定理 4. 命 $F(x)$ 表一无固定素因子的 k 次整值既約多項式，命

$$n = \begin{cases} k+1, & \text{若 } 1 \leqslant k \leqslant 5; \\ k+w, & \text{若 } k > 5, \end{cases}$$

此处 w 是适合下面不等式的最小正整数:

$$w+1 \geqslant \frac{5.64527}{4.8396}+\frac{3.65}{4.8396} \log \frac{5k-w}{w+5},$$

则在貫 $\{F(x)\}$ 中存在无限多个不超过 n 个素数的乘积.

特别,由此可知,存在无限多个 x,使 x^2+1 为不超过 3 个素数的乘积.

定理 5. 当 x 充分大时,则

(i) 在区間 $x<n \leqslant x+x^{\frac{10}{17}}$ 中,恆有一个整数,它不超过 2 个素数的乘积;

(ii) 在区間 $x<n \leqslant x+x^{\frac{20}{49}}$ 中,恆有一个素因子个数不多于 3 的整数.

2. 特征和及其应用

利用 Weil 关于有限代数函数体上的 Riemann 猜想的結果(見 § 12), Burgess[7]証明了:

命 δ, ε 为任何正数,则当 $H>p^{\frac{1}{4}+\delta}$ 及 p 充分大时,对任何整数 N,都有

$$\left|\sum_{n=N+1}^{N+H}\left(\frac{n}{p}\right)\right|<\varepsilon H,$$

此处 $\left(\frac{n}{p}\right)$ 表示 Kronecker 符号.

由此他推出了

定理 1. 命 $N_{\min}$ 表示模 p 的最小正二次非剩余,则

$$N_{\min}=O\left(p^{\frac{1}{4\sqrt{e}}+\varepsilon}\right),$$

此处与"O"有关的常数仅依赖于 ε.

王元[8] 首先根据 Burgess 的方法,加以改变,从而把他的結果推广并改进为(参看 Burgess[9])

定理 2. 命 δ 为不超过 $\frac{1}{6}$ 的一个正数,则当 $p>P(\delta)$ 及 $H>p^{\frac{1}{4}+\delta}$ 时,对任何整数 N,都有

$$\left|\sum_{n=N+1}^{N+H} \chi(n)\right|<\frac{H}{p^{\eta}},$$

此处 $\eta=\frac{\delta^2}{6}$,而 χ 为模 p 的非主特征.

以此与 Brun 的篩法相結合,就得到

定理 3. 命 $g(p)$ 表示模 p 的最小正原根,则

$$g(p)=O\left(p^{\frac{1}{4}+\varepsilon}\right),$$

此处 ε 为任何正数,而与 O 有关的常数仅依赖于 ε.

对于整数 $H > 0$, $q > 0$, t, N,定义区間 $I(q, t)$:

$$\frac{N + tp}{q} < z \leqslant \frac{N + H + tp}{q}.$$

引. 若集合 Φ 表示含有 Q 个两两互素的整数的集合, Φ 中的元素 q 还满足:

$$q_1 < q < q_2, \quad 2Hq_2 < p.$$

当給了 p, N, H 后,对于每个 $q \in \Phi$,有 t 的集合 $T(q)$,此处 $0 \leqslant t < q$, $T(q)$ 共 $q - Q$ 个元素. 对于 Φ 中的全体 q 及 $T(q)$ 中的全体 t,区間 $I(q, t)$ 之間沒有公共整数.

定理 2 的証明: 1) 記 $S_h(x) = \sum_{m=1}^{h} \chi(x + m)$. 若 χ 为模 p 的 d 次特征,则

$$\sum_x |S_h(x)|^{2r} =$$

$$= \sum_{m_1=1}^{h} \cdots \sum_{m_r=1}^{h} \sum_{n_1=1}^{h} \cdots \sum_{n_r=1}^{h} \sum_x \chi((x+m_1)\cdots(x+m_r)) \cdot \bar{\chi}((x+n_1)\cdots(x+n_r)).$$

将諸 $\{m_1, \cdots, m_r; n_1, \cdots, n_r\}$ 分成两类 σ_1 与 σ_2; σ_1 的元素满足: $m_{i_1} = n_{j_1}, \cdots, m_{i_s} = n_{j_s}$, $\{m_{i_{s+1}}, \cdots, m_{i_r}\}$ 及 $\{n_{j_{s+1}}, \cdots, n_{j_r}\}$ 中每个数的重复次数都是 d 的倍数,此处 $(i_1, \cdots, i_r)$ 及 $(j_1, \cdots, j_r)$ 都是 $(1, \cdots, r)$ 的排列. 其余的都属于 σ_2. 因此

$$\sum_x |S_h(x)|^{2r} = \sum_{\sigma_1} \sum_x \chi((x+m_1)\cdots(x+m_r))\bar{\chi}((x+n_1)\cdots(x+n_r)) +$$

$$+ \sum_{\sigma_2} \sum_x \chi((x+m_1)\cdots(x+m_r))\bar{\chi}((x+n_1)\cdots(x+n_r)) =$$

$$= \Sigma_1 + \Sigma_2.$$

由于 σ_1 的元素个数少于 $(2r)^{7r}h^r$,故得

$$|\Sigma_1| < (2r)^{7r} p h^r.$$

又由 Weil 方法,可知

$$|\Sigma_2| < 2r\sqrt{p}\, h^{2r}.$$

因此

$$\sum_x |S_h(x)|^{2r} < (2r)^{7r} p h^r + 2r\sqrt{p}\, h^{2r}.$$

2) 由 Pólya 定理可知,不妨假定

$$p^{\frac{1}{4}+\delta} < H < p^{\frac{1}{2}+\delta}.$$

若定理不眞,卽有 H 及 N,使

$$\left| \sum_{n=N+1}^{N+H} \chi(n) \right| \geqslant \frac{H}{p^{\eta}}.$$

当 p 充分大时，我們将由此得到一个矛盾.

对于 $q < p$，有

$$\sum_{n=N+1}^{N+H} \chi(n) = \sum_{t=0}^{q-1} \sum_{z \in I(q,t)} \chi(z),$$

故得

$$\sum_{t=0}^{q-1} \left| \sum_{z \in I(q,t)} \chi(z) \right| \geqslant \frac{H}{p^{\eta}}.$$

应用引理，命 Φ 是适合 $p^{\frac{1}{4}} - \frac{p^{\frac{1}{4}}}{p^{\eta}} < q < p^{\frac{1}{4}}$ 的全体素数，则 Φ 的元素个数为 $Q = \frac{4p^{\frac{1}{4}-\eta}}{\log p} \times$ $\times (1 + o(1))$. 关于 q 求和，当 p 充分大时，得到

$$\sum_{I} \left| \sum_{z \in I} \chi(z) \right| = \sum_{q} \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi(z) \right| \geqslant \frac{HQ}{p^{\eta}} - \sum_{q} 2HQq^{-1} \geqslant \frac{HQ}{2p^{\eta}}.$$

由于 $I(q, t)$ 的个数不超过 $p^{\frac{1}{4}}Q$ 及

$$\sum_{n \in I} \sum_{m=1}^{h} \chi(x+m) = h \sum_{z \in I} \chi(z) + \theta h^2, \quad |\theta| \leqslant 2,$$

故得

$$\sum_{I} \sum_{n \in I} |S_h(n)| > \frac{HQh}{2p^{\eta}} - 2p^{\frac{1}{4}}Qh^2.$$

命

$$h = \left[\frac{Hp^{\frac{1}{4}}}{8p^{\eta}} \right],$$

则

$$\sum_{I} \sum_{n \in I} |S_h(n)| > \frac{HQh}{4p^{\eta}}.$$

由 Hölder 不等式得到

$$\sum_{I} \sum_{n \in I} |S_h(n)|^{2r} > \left(\frac{1}{4p^{\eta}} HQh \right)^{2r} (p^{\frac{1}{4}}Q \cdot 3p^{-\frac{1}{4}}H)^{1-2r} > \left(\frac{1}{12p^{\eta}} \right)^{2r} HQh^{2r},$$

故由引理可知

$$\sum_{x} |S_h(x)|^{2r} > \left(\frac{1}{12p^{\eta}} \right)^{2r} HQh^{2r}.$$

因此由 1) 得出

$$\left(\frac{1}{12p^{\eta}} \right)^{2r} HQh^{2r} < (2r)^{7r} p h^r + 2r\sqrt{p}\, h^{2r}.$$

命 $r = \left[\frac{2}{\delta} \right] + 1$. 当 p 充分大时，上式不可能，故得定理.

又在广义 Riemann 猜想下，王元[8] 用 Brun 篩法証明了

定理 4.

$$g(p) = O(m^6 \log^2 p),$$

此处 m 表示 $p-1$ 的互异的素因子个数.

运用定理 2，还可以得到模 p 的最小 n 次非剩余 $N(p, n)$ 的估計[10]如下:

定理 5. 任意給定 $\varepsilon > 0$,则当 p 充分大时,

(i) $N(p, n) \leqslant p^{\frac{1}{4e\frac{n-1}{n}}+\varepsilon}$ $(n \geqslant 2)$;

(ii) $N(p, n) \leqslant p^{\frac{1}{12}}$ $(n \geqslant 21)$;

(iii) $N(p, n) \leqslant p^{\frac{\log\log n+2}{4\log n}}$ $(n \geqslant e^{33})$;

(iv) 在广义 Riemann 猜想下, $N(p, n) = O(\log^2 p)$.

3. 素 数 定 理

我們将在这里証明

$$\pi(x) = \operatorname{li} x + O(xe^{-a(\log x)^{\frac{3}{5}+\varepsilon}}).$$

这里的方法基本上是 Виноградов 的, Коробов[11]也証明了此同一結果.

由第二章 §9 定理 1 立刻得出

引. 設 $b \geqslant \frac{1}{4}k(k+1)+lk$, $P>2$ 为一整数, 则对任意給定的一組整数 $z_1, \cdots, z_k$,方程組

$$\xi_1^s + \cdots + \xi_b^s - \xi_{b+1}^s - \cdots - \xi_{2b}^s = z_s \quad (1 \leqslant s \leqslant k)$$

的整数解組数不超过

$$(7b)^{4bl} P^{2b-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)\left(1-\frac{1}{k}\right)^l} (\log P)^{2l}.$$

我們将証明以下的定理,由此定理与經典的方法,就得到上述的关于素数定理的結果.

定理. 設 $k \geqslant 7$, $k_0 = \left[\frac{k}{6}\right]$, $k_1 = \delta k$; a, a_1 为二整数, $a \geqslant e^{5000k_1^2}$, $a < a_1 \leqslant$ $\leqslant 2a$. 又設 $t = a^{k-\theta}$, $0 < \theta \leqslant 1$,

$$S = \sum_{a<n\leqslant a_1} e^{2\pi i f(n)}, \quad f(n) = \frac{-t\log n}{2\pi},$$

则

$$|S| \leqslant 1.7a^{1-\frac{1}{42\cdot 10^6 k^2}}.$$

証. 命 $P = [a^{\frac{3}{4}}]$, $Q = [a^{\frac{1}{8}}]$,易見

$$S = \frac{1}{PQ}\sum_{x=1}^{P}\sum_{y=1}^{Q}\sum_{a<n\leqslant a_1} e^{2\pi i f(n)} = \frac{1}{PQ}\sum_{a<n\leqslant a_1} S_n + 2\theta' a^{\frac{7}{8}},$$

此处 $|\theta'| \leqslant 1$,

$$S_n = \sum_{x=1}^{P} \sum_{y=1}^{Q} e^{2\pi i f(n+xy)}.$$

将 $f(n + xy)$ 展开,而命 $A_0 = f(n)$, $A_s = \frac{(-1)^s t}{2\pi s n^s}\ (s > 0)$,

$$\psi(x, y) = A_0 + A_1 xy + \cdots + A_{k_1} x^{k_1} y^{k_1},$$

则有

$$|f(n + xy) - \psi(x,y)| \leqslant \frac{a^{-\frac{1}{8}}}{16\pi k}.$$

于是

$$S_n = S_n' + \frac{\theta''}{7k} PQa^{-\frac{1}{8}},$$

此处 $|\theta''| < 1$, 而

$$S_n' = \sum_{x=1}^{P} \sum_{y=1}^{Q} e^{2\pi i \psi(x, y)}.$$

因此

$$S = \frac{1}{PQ} \sum_{a<n\leqslant a_1} S_n' + 3\theta''' a^{\frac{7}{8}}, \tag{10}$$

θ''' 也是一絕对值小于 1 的数.

命 $r = 2b$, $r_0 = 2b_0$,

$$b = \left[9k_1^2 + \frac{k_1(k_1 + 1)}{4} + 1\right], \quad b_0 = \left[7k_1^2 + \frac{k_1(k_1 + 1)}{4} + 1\right].$$

用二次 Hölder 不等式得到

$$|S_n'|^{r_0 r} \leqslant \left(P^{r_0-1} \sum_{x} \sum_{y_1} \cdots \sum_{y_{r_0}} e^{2\pi i\left(A_1 x Y_1' + \cdots + A_{k_1} x^{k_1} Y_{k_1}'\right)}\right)^r \leqslant$$

$$\leqslant P^{(r_0-1)r} Q^{r_0(r-1)} \sum_{y_1} \cdots \sum_{y_{r_0}} \sum_{x_1} \cdots \sum_{x_r} e^{2\pi i\left(A_1 Y_1' x_1 + \cdots + A_{k_1} Y_{k_1}' x_{1 k_1}\right)},$$

式中

$$X_s = x_1^s + \cdots + x_b^s - x_{b+1}^s - \cdots - x_r^s \quad (1 \leqslant s \leqslant k_1),$$

$$Y_s' = y_1^s + \cdots + y_{b_0}^s - y_{b_0+1}^s - \cdots - y_{r_0}^s \quad (1 \leqslant s \leqslant k_1).$$

X_s 只能取得 $-bP^s < z_s \leqslant bP^s$ 中的数值. 对于一組 $z_1, \cdots, z_{k_1}$, 方程組 $X_1 = z_1$, $\cdots$, $X_{k_1} = z_{k_1}$ 的整数解組数不超过 U,此处

$$U = U_0 P^{r - \frac{1}{2}k_1(k_1+1) + \frac{1}{2}k_1(k_1+1)\left(1 - \frac{1}{k_1}\right)^{9k_1}} (\log a)^{18k_1}, \quad U_0 = (7b)^{36bk_1}.$$

于是

$$|S_n'|^{r_0 r} \leqslant P^{(r_0-1)r} Q^{r_0(r-1)} U \sum_{z_1} \cdots \sum_{z_{k_1}} \left| \sum_{y_1} \cdots \sum_{y_{r_0}} e^{2\pi i\left(A_1 Y_1' z_1 + \cdots + A_{k_1} Y_{k_1}' z_{k_1}\right)} \right|.$$

再經过一次 Hölder 不等式得到

$$|S_n'|^{2r_0r} \leqslant P^{2(r_0-1)r}Q^{2r_0(r-1)}U^2r^{k_1}P^{\frac{1}{2}k_1(k_1+1)}\sum_{x_1}\cdots\sum_{x_{k_1}}\sum_{y_1}\cdots\sum_{y_{2r_0}} e^{2\pi i(A_1Y_1x_1+\cdots+A_{k_1}Y_{k_1}x_{k_1})},$$

此处

$$Y_s = y_1^s + \cdots + y_{r_0}^s - y_{r_0+1}^s - \cdots - y_{2r_0}^s \quad (1 \leqslant s \leqslant k_1),$$

它只能取得 $-r_0Q^s < \eta_s < r_0Q^s$ 中的数值. 对于一組 $\eta_1, \cdots, \eta_{k_1}$,方程組 $Y_1 = \eta_1, \cdots, Y_{k_1} = \eta_{k_1}$ 的解数不超过

$$W = W_0Q^{2r_0-\frac{1}{2}k_1(k_1+1)+\frac{1}{2}k_1(k_1+1)\left(1-\frac{1}{k_1}\right)^{7k_1}}(\log a)^{14k_1}, \quad W_0 = (7r_0)^{28r_0k_1}.$$

于是

$$|S_n'|^{2r_0r} \leqslant P^{2(r_0-1)r}Q^{2r_0(r-1)}U^2r^{k_1}P^{\frac{1}{2}k_1(k_1+1)}W\sum_{\eta_1}\cdots\sum_{\eta_{k_1}}H_1\cdots H_{k_1}, \tag{11}$$

此处

$$H_s = \left|\sum_{x_s} e^{2\pi iA_s\eta_sx_s}\right|.$$

如果用最粗糙的估計 $H_s \leqslant rP^s$,将得

$$\sum_{\eta_1}\cdots\sum_{\eta_{k_1}}H_1\cdots H_{k_1} \leqslant (2r_0r)^{k_1}(PQ)^{\frac{1}{2}k_1(k_1+1)} = D. \tag{12}$$

为了得到更精密的估計,我們将 $(\eta_1, \cdots, \eta_{k_1})$ 分成二类: E_1 与 E_2. 对于落入 E_1 中的 $(\eta_1, \cdots, \eta_{k_1})$, 在 $\eta_{k+k_0+1}, \cdots, \eta_{k+k_0+2k}$ 中至少有 k 个 η 等于 0, 而将无此性質的 $(\eta_1, \cdots, \eta_{k_1})$ 都归入 E_2. 显然我們有

$$\sum_{(\eta_1,\cdots,\eta_{k_1})\in E_1}\cdots\sum H_1\cdots H_{k_1} \leqslant r^{k_1}P^{\frac{1}{2}k_1(k_1+1)}\sum_{(\eta_1,\cdots,\eta_{k_1})\in E_1}\cdots\sum 1 \leqslant$$

$$\leqslant r^{k_1}P^{\frac{1}{2}k_1(k_1+1)}(2r_0)^{k_1}Q^{\frac{1}{2}k_1(k_1+1)}\frac{\binom{2k}{k}(2r_0)^kQ^{(k+k_0+k+1)+\cdots+(k+k_0+2k)}}{(2r_0)^{2k}Q^{(k+k_0+1)+\cdots+(k+k_0+2k)}} \leqslant$$

$$\leqslant DQ^{-k^2} \leqslant Da^{-\frac{1}{8}k^2}.$$

又若 $\eta_s \neq 0(k + k_0 + 1 \leqslant s \leqslant k + k_0 + 2k)$,則因

$$|A_s\eta_s| \leqslant \frac{tr_0Q^s}{2\pi sn^s} < \frac{b_0Q^{k+k_0+1}}{\pi ka^{k_0+1}} < \frac{b_0}{\pi k}a^{\frac{1}{8}k-\frac{7}{8}(k_0+1)} < 0.1,$$

故有

$$\frac{H_s}{rP^s} \leqslant \frac{1}{2|A_s\eta_s|rP^s} \leqslant \frac{2\pi s2^sa^s}{2rtP^s} \leqslant \frac{10k_02^sa^{\frac{3}{4}s+1-k}}{r} < \frac{1}{2}a^{-\frac{k}{16}}.$$

因为对于 E_2 中的 $(\eta_1, \cdots, \eta_{k_1})$, 至少有 k 个 $\eta_s(k + k_0 + 1 \leqslant s \leqslant k + k_0 + 2k)$ 不等于 0,因此

$$\sum_{(\eta_1,\cdots,\eta_{k_1})\in E_2}\cdots\sum H_1\cdots H_{k_1} \leqslant \frac{1}{2}Da^{-\frac{k^2}{16}}.$$

于是我們得到比(12)更精密的估計

$$\sum_{\eta_1} \cdots \sum_{\eta_{k_1}} H_1 \cdots H_{k_1} \leqslant D a^{-\frac{k^2}{16}}.$$

由此得出

$$|S_n'|^{2r_0r} \leqslant (PQ)^{2r_0r} P^{k_1(k_1+1)\left(1-\frac{1}{k_1}\right)^{9k_1}} Q^{\frac{1}{2}k_1(k_1+1)\left(1-\frac{1}{k_1}\right)^{7k_1}} a^{-\frac{k^2}{16}} (\log a)^{50k_1} (2r_0r^2)^{k_1} U_0^2 W_0. \quad (13)$$

因为

$$P^{k_1(k_1+1)\left(1-\frac{1}{k_1}\right)^{9k_1}} Q^{\frac{1}{2}k_1(k_1+1)\left(1-\frac{1}{k_1}\right)^{7k_1}} \leqslant a^{\left(\frac{3}{4}e^{-9}+\frac{1}{16}e^{-7}\right)k_1(k_1+1)} \leqslant a^{0.009761k^2},$$

$$(\log a)^{50k_1} = a^{50k_1\frac{\log\log a}{\log a}} \leqslant a^{\frac{\log(5000\ k_1)}{100\ k_1}} \leqslant a^{0.000062k^2}.$$

而

$$0.009761 + 0.000062 - \frac{1}{16} \leqslant -\frac{1}{19};$$

又有

$$(2r_0r^2)^{k_1} \leqslant (8b_0b^2)^{k_1} < e^{k_1 \log 5060 + 6k_1 \log k_1},$$

$$U_0^2 W_0 \leqslant (70k_1^2)^{720k_1^3} (105k_1^2)^{420k_1^3} \leqslant e^{(720 \log 70 + 420 \log 105 + 2280 \log k_1)\, k_1^3},$$

$$2r_0r \geqslant 536.5k_1^4,$$

而

$$\frac{(\log 5060 + 6\log k_1)k_1 + (720\log 70 + 420\log 105 + 2280\log k_1)k_1^3}{536.5k_1^4} \leqslant \frac{1}{2},$$

故由(13)得到

$$|S_n'| \leqslant PQa^{-\frac{k^2}{19\cdot 536.5k_1^4}} e^{\frac{1}{2}} \leqslant 1.7\ PQa^{-\frac{1}{42\cdot 10^6\, k^2}}.$$

由此与(10)得出定理，明所欲証.

4. $G(k)$ 的最新結果

Виноградов[12]在 1959 年将 $G(k)$ 的上界改进为：对于充分大的 k,

$$G(k) < k(2\log k + 4\log\log k + 2\log\log\log k + 13). \quad (14)$$

他的方法主要是引进一个新的数集 $\{w\}$，以代替第四章 § 26 中的集合 $\{u_0\}$，然后用一个对应的三角和估計(下文中的引 5)来代替 § 26 的引理 2.

我們需要以下一些引理.

引 1. 設 a, b, P, Q 都是整数, $P > 0$, $Q > 0$, $\Phi(y)$ 为 y 的实函数,

$$S = \sum_{x=a}^{a+P-1} \sum_{y=b}^{b+Q-1} \xi(x)\eta(y) e^{2\pi i x \Phi(y)},$$

$$\sum_{x=a}^{a+P-1} |\xi(x)|^2 = K, \quad \sum_{y=b}^{b+Q-1} |\eta(y)| = L, \quad \max_y |\eta(y)| = \eta.$$

(a) 若

$$\Phi(y)=\frac{hy+\psi(y)}{q},\quad (h,q)=1,\ q>0,\ \lambda\geqslant 0,$$

且当 y 經过 $\leqslant q$ 个相継的整数时，$\psi(y)$ 的最大值与最小值之差不超过 λ，則

$$|S|<\sqrt{KL\eta[(2\lambda+6)P+3q](Qq^{-1}+1)}.$$

(b) 若对任何 y，

$$\frac{1}{A}\leqslant\Phi(y+1)-\Phi(y)\leqslant\frac{\beta}{A},$$

此处 $A\geqslant 2\beta>2$，則

$$|S|<\sqrt{KL\eta(4P+3A)(Q\beta A^{-1}+1)}.$$

見 Виноградов 著"数論中的三角和法"第一章引理 10b 及 10c.

引 2. 設 P 为一充分大的整数，$Q=[\sqrt{P}]$，$|z_s|\leqslant c_sQ^s$，c_s 与 Q 无关. 又設 $1\leqslant l\leqslant k$，則对确定的 B_l 值，

$$B_l=P^{k-1}z_1+\cdots+P^{k-l}z_l \tag{15}$$

的整数解 $(z_1,\cdots,z_l)$ 的組数

$$\ll Q^{\frac{l(l+1)}{2}-1}P^{-l+1}.$$

証. 当 $l=1$ 时，显然眞确.

假設于 $l-1$ 时引理成立. 命 $(z_1,\cdots,z_l)$ 与 $(z_1',\cdots,z_l')$ 为方程(15)的任意两組解答，則有

$$P^{k-1}z_1+\cdots+P^{k-l+1}z_{l-1}-P^{k-1}z_1'-\cdots-P^{k-l+1}z_{l-1}'=$$
$$=P^{k-l}(z_l'-z_l)\ll P^{k-l}Q^l.$$

所以 $P^{k-1}z_1+\cdots+P^{k-l+1}z_{l-1}$ 与 $P^{k-1}z_1'+\cdots+P^{k-l+1}z_{l-1}'$ 必須同落在一个长为 $O(P^{k-l}Q^l)$ 的区間中. 又在此区間中，含有 $O\left(\frac{P^{k-l}Q^l}{P^{k-l+1}}\right)$ 个 B_{l-1} 值，于是由数学归納法的假定可知，$(z_1,\cdots,z_{l-1})$ 的組数

$$\ll\frac{P^{k-l}Q^l}{P^{k-l+1}}Q^{\frac{l(l-1)}{2}-1}P^{-(l-1)+1}\ll Q^{\frac{l(l+1)}{2}-1}P^{-l+1};$$

而在取定 $(z_1,\cdots,z_{l-1})$ 后，z_l 也就唯一确定. 引理得証.

引 3. 設 $n<k$ 为一整数，$r_1=[1.6n^2\log n]$，$r=2r_0=4r_1$. 命

$$A=(P+y_1)^k+\cdots+(P+y_{r_0})^k-(P+y_{r_0+1})^k-\cdots-(P+y_r)^k,$$

其中 $y_1,\cdots,y_r$ 各自独立地跑过 $1,\cdots,Q$，則至多有

$$Q^{r+\varepsilon}P^{-n/2}$$

組 $(y_1,\cdots,y_r)$，使 A 落在一确定的长为 $O(P^{k-\frac{n+1}{2}})$ 的区間内.

證. 命

$$\eta_s = y_1^s + \cdots + y_{r_0}^s - y_{r_0+1}^s - \cdots - y_r^s \quad (1 \leqslant s \leqslant k)$$

及 $U_s = \binom{k}{s}\eta_s$,則有 $-r_0k^sQ^s < U_s \leqslant r_0k^sQ^s$,而

$$A = P^{k-1}U_1 + \cdots + PU_{k-1} + U_k.$$

因为

$$P^{k-n-1}U_{n+1} + \cdots + PU_{k-1} + U_k \ll P^{k-\frac{n+1}{2}},$$

故若 A 落在一长为 $O(P^{k-\frac{n+1}{2}})$ 的区間中,則

$$P^{k-1}U_1 + \cdots + P^{k-n}U_n$$

也如此;而由引理 2 可知,使

$$B_n = P^{k-1}z_1 + \cdots + P^{k-n}z_n$$

落在一长为 $O(P^{k-\frac{n+1}{2}})$ 的区間中的 $(z_1, \cdots, z_n)$ 組数

$$\ll \frac{P^{k-\frac{n+1}{2}}}{P^{k-n}} Q^{\frac{n(n+1)}{2}-1} P^{-n+1} \ll Q^{\frac{n(n+1)}{2}} P^{-\frac{n}{2}}.$$

又因 $r > 2n^2(3\log n + \log\log n + 4) - 4$ (n 充分大时),故对每一組 $(z_1, \cdots, z_n)$,由第二章 §9 定理 3 可知,方程組

$$U_1 = z_1, \ \cdots, \ U_n = z_n$$

的解 $(y_1, \cdots, y_r)$ 的組数 $\ll Q^{r-\frac{1}{2}n(n+1)+\varepsilon}$. 于是得到引理.

今設 k 为一整数,N 为一充分大的整数,

$$P_0 = [N^{\frac{1}{k}}], \quad P_1 = [\sqrt{P_0}], \quad Q_1 = [\sqrt{P_1}], \quad R = [P_1^{1-\frac{1}{2k}}],$$

$$\tau = 2kP_0^{k-1}, \quad \tau_0 = P_1^{k-\frac{1}{2}}, \quad \beta = \frac{1}{4}\left(1 - \frac{1}{2k}\right).$$

区間 $-\tau_0^{-1} \leqslant \alpha < 1 - \tau_0^{-1}$ 中的 α 都能表成

$$\alpha = \frac{h}{q} + z, \ (q, h) = 1, \ 0 < q \leqslant \tau_0, \ 0 \leqslant h < q, \ |z| \leqslant \frac{1}{q\tau_0}$$

的形状. 用 $\mathfrak{M}_{h,q}$ 表示区間

$$\left|\alpha - \frac{h}{q}\right| \leqslant \frac{1}{q\tau}, \quad (h, q) = 1, \quad q \leqslant P_0^\beta.$$

而用 E 表示在 $-\tau_0^{-1} \leqslant \alpha < 1 - \tau_0^{-1}$ 中除去一切 $\mathfrak{M}_{h,q}$ 后所剩余的部分. 不难証明,所有的 $\mathfrak{M}_{h,q}$ 互不相交.

又設 $n(<k)$, $n'(>2k)$ 为二整数,命 $\delta = \left(k - \frac{n+1}{2}\right)\Big/\left(k - \frac{1}{2}\right)$,

$$P_i = [P_1^{\delta^{i-1}}], \quad Q_i = [\sqrt{P_i}] \quad (2 \leqslant i \leqslant n_2).$$

引 4. 命

$$A_i=(P_i+y_{i_1})^k+\cdots+(P_i+y_{ir_0})^k-(P_i+y_{i,r_0+1})^k-\cdots-(P_i+y_{ir})^k,$$

$y_{i_1},\cdots,y_{ir}$ 各自独立地經过 $1,\cdots,Q_i(1\leqslant i\leqslant n')$,則至多有

$$\ll(Q_1Q_2\cdots Q_{n'})^{r+\varepsilon}P_1^{-\left(k-\frac{1}{2}\right)(1-\delta^{n'})}$$

組 $(y_{11},\cdots,y_{1r},\cdots,y_{n'1},\cdots,y_{n'r})$,使

$$W=A_1+A_2+\cdots+A_{n'}$$

落在一确定的长为 $O(P_{n'}^{k-\frac{n+1}{2}})$ 的区間中.

証. 显然 $A_i\ll Q_iP_i^{k-1}\ll P_{i-1}^{k-\frac{n+1}{2}}(2\leqslant i\leqslant n')$,故若 W 落在此区間中,則 A_1 将落在一长为 $O(P_1^{k-\frac{n+1}{2}})$ 的区間中,而由引 3 可知,$(y_{11},\cdots,y_{1r})$ 的組数 $\ll Q_1^{r+\varepsilon}P_1^{-n/2}$;又对一組确定的 $(y_{11},\cdots,y_{1r})$,根据同样的理由,A_2 将落在一长为 $O(P_2^{k-\frac{n+1}{2}})$ 的区間中,所以 $(y_{21},\cdots,y_{2r})$ 的組数 $\ll Q_2^{r+\varepsilon}P_2^{-n/2}$; $\cdots$; 等等,而得引理.

引 5. 命

$$W(\alpha)=\sum_p\sum_w e^{2\pi i\alpha p^k w},$$

和号中的 p 經过 $R<p\leqslant 2R$ 中的全体素数,而 w 則經过形如

$$(P_1+y_1)^k+\cdots+(P_{n'}+y_{n'})^k$$

的数,而 $y_i(1\leqslant i\leqslant n')$ 則分別独立地通过 $1,\cdots,Q_i$. 于是当 $\alpha\in E$ 时,可有

$$W(\alpha)\ll W(0)P_1^K,\quad K=\frac{1}{r_0}\left[-\frac{1}{4}\left(1-\frac{1}{2k}\right)+\frac{1}{2}\left(k-\frac{1}{2}\right)\delta^{n'}+\varepsilon k\right].$$

証. 用 Hölder 不等式得到

$$|W(\alpha)|^{r_0}\ll R^{r_0-1}|T(\alpha)|,\quad T(\alpha)=\sum_p\sum_x\xi(x)e^{2\pi i\alpha p^k x},$$

此处 $\xi(x)$ 为

$$w_1+\cdots+w_{r_1}-w_{r_1+1}-\cdots-w_{r_0}=x$$

的解 $(y_1,\cdots,y_{n'})$ 的組数,显然有 $x\ll P_1^{k-\frac{1}{2}}$.

因为 $\alpha\in E$,故若将 α 表成 $\alpha=\frac{h}{q}+z,(h,q)=1$,那末或者 (i) $P_0^\beta<q\leqslant\tau_0$, $|z|\leqslant\frac{1}{q\tau_0}$;或者 (ii) $q\leqslant P_0^\beta,\frac{1}{q\tau}<|z|\leqslant\frac{1}{q\tau_0}$.

对于(i),用 $p_1(y),\cdots,p_{\rho(y)}(y)$ 表示 $R<p\leqslant 2R$ 中适合 $p^k\equiv y\pmod q$ 的全体素数;而命 $\rho=\max\limits_{0\leqslant y\leqslant q-1}\rho(y)$ 及 $\eta_j(y)=1$ (假如 $j\leqslant\rho(y)$), $=0$ (假如 $j>\rho(y)$),于是

$$T(\alpha)=\sum_{j=1}^{\rho}\sum_x\sum_{y=0}^{q-1}\xi(x)\eta_j(y)e^{2\pi ix\frac{hy+\psi(y)}{q}},$$

此处 $\psi_j(y)=qzp_j^k(y)$,因为 $\sum\limits_x|\xi(x)|^2$ 即

$$w_1 + \cdots + w_{r_0} - w_{r_0+1} - \cdots - w_r = 0$$

的解数,故由引 4 可知,引 1 中的

$$K \ll (Q_1 \cdots Q_{n'})^{r+\varepsilon} P_1^{-\left(k-\frac{1}{2}\right)(1-\delta^{n'})};$$

又易見 $L = \sum_y |\eta_i(y)| \leqslant \min(R, q)$, $\eta = 1$, $\lambda = 1$, $\rho \ll \left(\frac{R}{q}+1\right) q^{\varepsilon}$, 于是由引 1(a)得到

$$T(\alpha) \ll \left(\frac{R}{q}+1\right) q^{\varepsilon} \sqrt{(Q_1 \cdots Q_{n'})^{r+\varepsilon} P_1^{-\left(k-\frac{1}{2}\right)(1-\delta^{n'})} \min(R,q) P_1^{k-\frac{1}{2}}} \ll$$

$$\ll R(Q_1 \cdots Q_{n'})^{r_0} P_1^{-\frac{1}{4}\left(1-\frac{1}{2k}\right)+\frac{1}{2}\left(k-\frac{1}{2}\right)\delta^{n'}+\varepsilon k}. \tag{16}$$

又对(ii),記 $p = qt + s$; 又根据 $qt + s$ 之为素数或否,定义 $\eta_s(t) = 1$ 或 0. 于是

$$T(\alpha) = \sum_{s=0}^{q-1} \sum_x \sum_{t > \frac{R-s}{q}}^{\leqslant \frac{2R-s}{q}} \xi(x) \eta_s(t) e^{2\pi i x \Phi_s(t)},$$

此处 $\Phi_s(t) = \frac{h}{q} s^k + z(qt+s)^k$. 因为

$$(R/P_0)^{k-1} \ll \Phi_s(t+1) - \Phi_s(t) \ll R^{k-1} P_1^{-k+\frac{1}{2}},$$

故由引 1(b) 得到

$$T(\alpha) \ll q \sqrt{(Q_1 \cdots Q_{n'})^{r+\varepsilon} P^{-\left(k-\frac{1}{2}\right)(1-\delta^{n'})} \left(\frac{R}{q}+1\right) \left[P_1^{k-\frac{1}{2}} + \left(\frac{P_0}{R}\right)^{k-1} \right]},$$

由此也能得出不等式(16). 引理得証.

如在第四章 § 26 中那样的定义 $T(\alpha)$, $T_i(\alpha)$ $(0 \leqslant i \leqslant m+1)$, $Q(\alpha)$ 及 $R(\alpha)$, 但需将那里的 P 换成 P_0. 由引 5 我們得到

$$\int_E T(\alpha)^{2k+1} R^2(\alpha) W(\alpha) e^{-2\pi i \alpha N} d\alpha \ll P^{2k+1} \max_{\alpha \in E} |W(\alpha)| \int_0^1 |R(\alpha)|^2 d\alpha \ll$$

$$\ll P_0^{2k+1+\varepsilon} W(0) P_0^{\frac{K}{2}} R(0) \ll P^{k+1} W(0) R^2(0) P_0^{\frac{K}{2}+k\left(1-\frac{1}{k}\right)^m+\varepsilon}.$$

如果取

$$n = [\log k], \quad n' = 3k, \quad m = [k(\log k + 2\log\log k + \log\log\log k + 3)],$$

容易証明:当 k 充分大时,

$$\frac{K}{2} + k\left(1-\frac{1}{k}\right)^m < 0.$$

于是

$$\int_E T(\alpha)^{2k+1} R^2(\alpha) W(\alpha) e^{-2\pi i \alpha N} d\alpha = o(P^{k+1} R^2(0) W(0)).$$

又因

$$\sum_{\mathfrak{M}_{h,q}}\int_{\mathfrak{M}_{h,q}} T(\alpha)^{2k+1}R^2(\alpha)W(\alpha)e^{-2\pi i\alpha N}d\alpha \gg P^{k+1}R^2(0)W(0),$$

故得

$$G(k) \leqslant 2k+1+2(m+3)+3k \leqslant$$
$$\leqslant 2k\log k + 4k\log\log k + 2k\log\log\log k + 11k + 7.$$

而得所需結果(14).

5. 其他問題

1. 关于素数定理(参看 § 5). P. Kuhn[13] 用 Selberg 的初等方法，算出了素数定理的誤差項. 他証明了

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^{1.1} x}\right)$$

以后，Левин[14] 又将这結果推广到算术級数中的素数定理，他証明了：当 $(l, q) = 1$ 时，

$$\pi(x, q, l) = \frac{x}{\varphi(q)\log x} + O\left(\frac{x}{\log^{1.14} x}\right).$$

2. 关于相継二素数之差距(参看 § 21). 尹文霖[15]指出，可以証明

$$\zeta\left(\frac{1}{2}+it\right) = O(|t|^{\frac{13}{80}+\varepsilon}),$$

从而推出了

$$p_{n+1} - p_n = O(n^{\frac{33}{53}+\varepsilon}).$$

3. 关于算术級数中的最小素数(参看 § 22). 潘承洞[16]計算出 Линник 結果

$$p(q, l) = O(q^c)$$

中的常数 c 适合 $c \leqslant 5448$；換句話説，他証明了

$$p(q, l) = O(q^{5448}).$$

4. 关于 Waring 問題(参看 §§ 25, 28). 关于 Waring 問題的优弧部分，华罗庚[17]証明：当 $s \geqslant k+1$ 时，

$$\sum_{\mathfrak{M}_{h,q}}\int_{\mathfrak{M}_{h,q}} T(\alpha)^s e^{-2\pi i N\alpha}d\alpha \sim \sigma(N)\frac{\Gamma\left(1+\frac{s}{k}\right)}{\Gamma\left(\frac{1}{k}\right)^s}N^{\frac{s}{k}-1}.$$

这一結果已臻于至善了. 这一結果的証明依賴于他[18]关于三角和的一个估計，即当 $k \geqslant 2$, $(h, q) = 1$ 时

$$\sum_{x=1}^{P} e^{2\pi i h x^k/q} = \frac{P}{q}\sum_{x=1}^{q} e^{2\pi i h x^k/q} + O(q^{\frac{1}{2}+\varepsilon}),$$

此处与O有关的常数仅依赖于ε及k.

此外,陈景潤証明了

$$37 \leqslant g(5) \leqslant 40^{[19]}$$

及

$$k \log k - k \leqslant g\left(\frac{x(x+1)\cdots(x+k-1)}{k!}\right) \leqslant 5(k \log k + 12)^{[20]}.$$

5. 关于Гольдбах問題(参看§31). 潘承洞[21]証明了:当N为大奇数时,

$$N = p_1 + p_2 + p_3,$$

此处

$$p_i = \frac{N}{3} + O(N^{\frac{139}{159}+\varepsilon}).$$

6. 关于一致分布(参看§37). Roth[22]証明了:对于任意貫$\{f(1)\}, \{f(2)\}, \cdots,$都有

$$\overline{\lim_{P\to\infty}} \bar{R}(P) \frac{1}{\sqrt{\log P}} \geqslant c > 0,$$

此处c为一絕对常数,而

$$\bar{R}(P) = \overline{\lim_{0\leqslant a<b\leqslant 1}} |N(P; a, b) - (b-a)P|.$$

7. 关于圓內整点問題与除数問題(参看§44). 关于圓內整点問題,陈景潤[23]証明了

$$A(x) = \pi x + O(x^{\frac{12}{37}+\varepsilon}).$$

关于除数問題,尹文霖[15]証明了

$$D(x) = x(\log x + 2\gamma - 1) + O(x^{\frac{13}{40}+\varepsilon}).$$

8. 关于几何数論的其他問題(参看§§46—47). 关于球內整点問題,Виноградов[25]証明了

$$\sum_{u^2+v^2+w^2\leqslant x} 1 = \frac{4}{3}\pi x^{3/2} + O(x^{\frac{19}{28}+\varepsilon})$$

以后,陈景潤[26]又証明了上式右端的誤差項可以换为

$$O(x^{\frac{35}{52}+\varepsilon}).$$

关于三維除数問題. 越民义[27]証明了

$$\alpha_3 \leqslant \frac{14}{29}$$

以后,尹文霖[28]及越民义与吳方[29]又依次将上面的結果改进为

$$\alpha_3 \leqslant \frac{10}{21}^{[28]} \quad 及 \quad \alpha_3 \leqslant \frac{8}{17}^{[29]}.$$

关于椭圓內的整点問題，吳方[30]建立了下面的漸近公式

$$\sum_{au^2+2buv+cv^2 \leqslant x} 1 = \frac{\pi x}{\sqrt{ac-b^2}} + O\left(x^{\frac{13}{40}+\varepsilon}\right),$$

此处 a, b, c 为实数，$a > 0$，$ac - b^2 > 0$。

补充参考資料

[1] 王元，表大偶数为两个殆素数之和，科学記录，1卷5期，267—270，1957；論篩法及其有关的若干应用(I)，数学学报，8卷3期，413—429，1958.

[2] 王元，論篩法及其有关的若干問題，科学記录，1卷1期，9—11，1957；表整数为素数及殆素数之和，数学学报，10卷2期，168—181，1960.

[3] М. Б. Барбан, Арифметическче функции на "Редких" Множествах, ДАН УзССР, 8, 10—12, 1961; новые применения "Большого решета" Ю. В. Линника, Тру. ин. Мат. им. В. И. Романовского, АН УзССР, 22, 1961.

[4] 潘承洞，表偶数为素数及殆素数之和，数学学报，12卷1期，95—106，1962.

[5] Wang Yuan (王元), On the representation of large integer as a sum of a prime and an almost prime, Scientia Sinica, Vol. XI, No. 8, 1—28, 1962.

[6] 王元，論篩法及其若干应用，科学記录，1卷3期，1—4，1957；論篩法及其有关的若干应用，数学学报，9卷2期，87—100，1959.

[7] D. A. Burgess, The distribution of quadratic residues and non-residues, Mathematica, London, 4, 106—112, 1957.

[8] 王元，关于素数的最小正原根，科学記录，3卷5期，135—139，1959，論素数的最小正原根，数学学报，9卷4期，432—441，1959.

[9] D. A. Burgess, On Character sums and primitive roots, Proc. Lond. Math. Soc. Vol. XII, No. 45, 179—192, 1962.

[10] 王元，关于模 p 的最小 n 次非剩余，(印刷中).

[11] Н. М. Коробов, Оценки тригонометрических сумм и их приложения, УМН СССР, **13**, 4, 185—192, 1958.

[12] И. М. Виноградов, К вопросу о верхней границе для $G(n)$, ИАН СССР, серия матем. **23**, 637—642, 1959.

[13] P. Kuhn, Eine Verbesserung des Restgliedes beim Beweis Primzahlsatzes, Math. Scand., **3**, 75—89, 1955.

[14] Б. В. Левин, К Вопросу о распределении простых уисел Арифметиуеской прогрессии, ИАН УзССР, серия матем., **5**, 15—28, 1961.

[15] 尹文霖，关于狄氏除数問題，科学記录新輯，**3**，131—134，1959；狄氏除数問題，北京大学学报(自然科学)，第2期，103—126，1959.

[16] 潘承洞，論算术級数中之最小素数，科学記录新輯，**1**，283—286，1957；論算术級数中之最小素数，北京大学学报(自然科学)，第4期，1—34，1956.

[17] 华罗庚，华林問題的优弧部分，科学記录新輯，**1**；3，15—16，1957.

[18] 华罗庚,关于指数和,科学記录新輯,**1**; 1, 1—4, 1957.
[19] 陈景潤,华林問題 $g(5)$ 的估計,科学記录新輯,**3**; 8, 259—265, 1959.
[20] 陈景潤,华林問題中 $g(\varphi)$ 的估計,数学学报,9 卷 3 期, 264—269, 1959.
[21] 潘承洞,堆垒素数論的一些新結果,数学学报,9 卷 3 期, 315—329, 1959.
[22] K. F. Roth, On irregularities of distribution, Mathematica, I, part 2. 73—79, 1954.
[23] 陈景潤,圓内整点問題,数学学报,13 卷 2 期, 299—313, 1963.
[24] И. М. Виноградов, К Вопросу о уисле целых тоуек в заданной области, ИАН СССР, серия Матем., **24**, 777—786, 1960.
[25] 陈景潤,給定区域内的整点問題,数学学报,12 卷 4 期, 408—420, 1962.
[26] 越民义,一个除数問題,数学学报,8 卷 4 期, 496—506, 1958.
[27] 尹文霖,关于三維除数問題,北京大学学报,第 3 期, 193—196, 1959.
[28] 越民义与吳方,关于三維除数問題,数学学报,12 卷 2 期, 170—174, 1960.
[29] 吳方,橢圓内的整点問題,数学学报 13 卷 2 期, 238—253, 1963.